



# HYBRID THREATS AND HYBRID WARFARE REFERENCE CURRICULUM



# HYBRID THREATS AND HYBRID WARFARE **REFERENCE CURRICULUM**



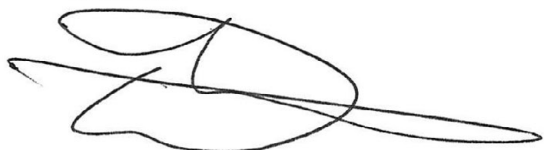
NATO Headquarters Brussels, June 2024



NATO Allies and partners are confronted with hybrid threats on a daily basis from state and non-state actors. They test our resilience and seek to exploit the openness, interconnectedness and digitalisation of our nations. They interfere in our democratic processes and institutions and target the security of our citizens, both directly and through proxies. They engage in sabotage, conduct malicious activities in cyberspace and space, promote disinformation campaigns, instrumentalise migration, manipulate energy supplies and employ economic coercion. These actors are also at the forefront of a deliberate effort to undermine multilateral norms and institutions and promote authoritarian models of governance.

It is essential that our decision makers, militaries and our populations are aware of these threats and challenges. Education and training activities are a key component in raising awareness. A reference curriculum on countering hybrid threats is an excellent vehicle for enhancing and strengthening practical cooperation in the framework of NATO's Partnerships, of which countering hybrid threats is an important component. It helps foster a shared understanding of the challenges we face.

I would like to commend the work of all those who participated in the development of this reference curriculum and wish you success in the training and education activities in which it is used.

A handwritten signature in black ink, consisting of several loops and a long horizontal stroke at the end.

David Van Weel,  
Assistant Secretary General  
Innovation, Hybrid and Cyber Division  
NATO HQ, Brussels





*"What is the object of defense? To preserve. To preserve is easier than to acquire."*

- Clausewitz: *On War* (1832) Book 6, Chapter 1

We, as NATO, are an alliance, founded on our shared values of democracy, freedom and sovereignty. In a world undergoing profound change, we see our democratic understanding and way of life increasingly challenged by authoritarian actors and their hybrid tactics.

NATO's decisiveness to consistently counter hybrid threats has increased and has been strengthened further since the Russian invasion. The Alliance has stressed that hybrid operations, to the extent that their effects are equivalent to a conventional attack, may lead to an invocation of Article 5. That is why NATO has gained knowledge and experience in dealing with hybrid tactics and has increased its situational awareness, strengthened its toolbox for countering hybrid threats and enhanced its Allies' resilience.

And still we must assume that hybrid threats will further intensify. As a result, in our first German National Security Strategy, we recognize the destructive potential that hybrid threats pose to society and democracy and have therefore announced a strategy aimed at increasing our capability to act in the face of these threats. This requires us to systematically understand hybrid tactics and to constantly develop our knowledge.

And this is where Partnership for Peace Consortiums can make a valuable contribution and provide a platform for knowledge sharing and collaboration. The curriculum supports our endeavor to counter hybrid threats as part of our efforts which we announced in the Brussels Summit Declaration of 2018 to support our partners in their fight against hybrid challenges. We therefore hope that we can make an educational contribution to this curriculum.

Dr Jasper Wieck

Director-General for Security and Defence Policy

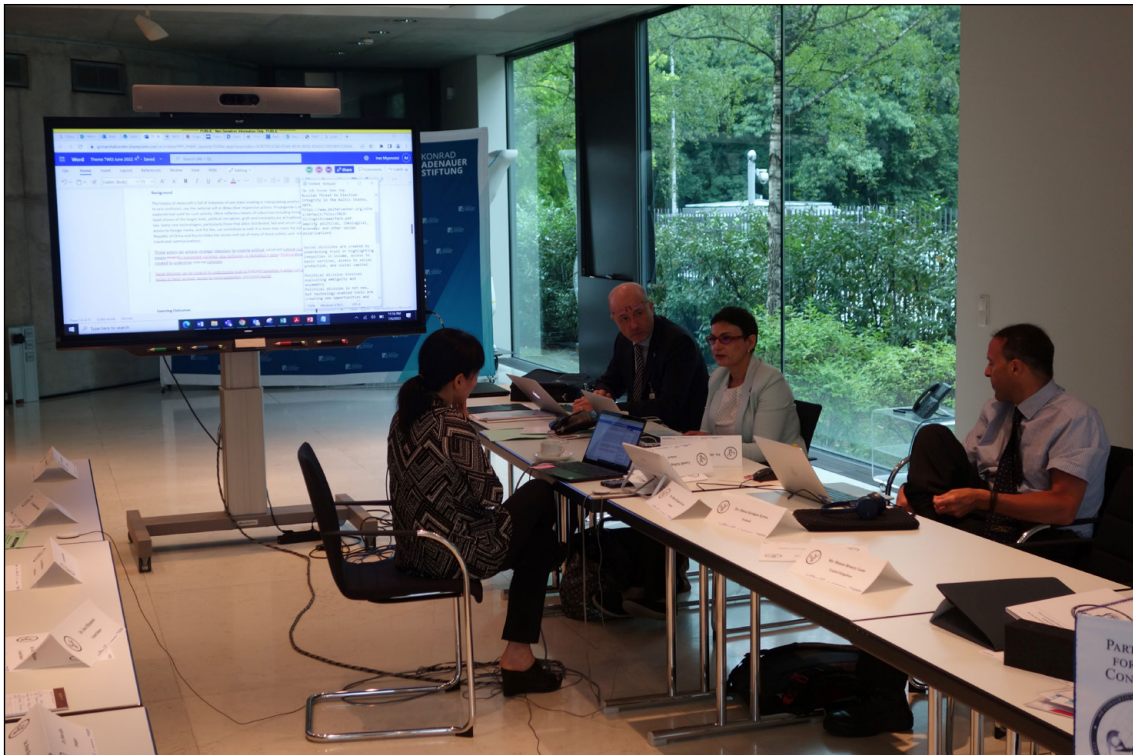
## About this Document

The Hybrid Threats and Hybrid Warfare Reference Curriculum (HTHWRC) is the result of a collaborative multinational team of volunteers brought together under the auspices of the Partnership for Peace Consortium of Defence Academies and Security Studies Institutes (PfPC) and its Emerging Security Challenges Working Group and with the generous funding of the German Federal Government. The cross functional group drafting this document included expert contributions from military, defence, academic and police officials. Our aim was to provide a well-rounded starting point for those who wish to explore or develop educational materials on the emerged and emerging challenges posed by hybrid threats and hybrid warfare activities present in the current security environment. We have taken a multi-disciplinary approach aimed at providing a framework to help learners develop the base knowledge and skills needed to understand these complex issues in order to successfully identify, anticipate and mitigate these potential threats.

We are grateful for the generous financial support of the German Federal Government and the very active support of the Defence Education Enhancement Programme (DEEP) of NATO and the PfPC central staff, EDWC Working Group, and Co-Chairs of the ESC Working Group, especially the leadership of Mr. Michael Gaul and LTC Olaf Garlich for their steadfast support. We also acknowledge the support provided by the Konrad Adenaur Foundation, the George C. Marshall Euro-

pean Center for Security Studies, the Robert Schuman Centre for Advanced Studies-European University Institute, the Ministry of Foreign Affairs, Republic of China, the New School (New York) University, and the [US] National Intelligence University – all of which made personnel, services or facilities available for this project. The co-editors wish to particularly acknowledge the group discussion leaders, Dr. Namrata Goswami, Dr. Everita Silina, Dr. Aleks Nesic and Dr. Todor Tagarev. This project would not have come to fruition without their keen participation as well as that of the many contributors who stayed with this long effort throughout – as listed at the end of this document. The editors thank everyone for their efforts but take responsibility for any errors or omissions with the final product.

Dr. Sean S. Costigan and Dr. Michael A. Hennessy  
HTHWRC Project Lead Authors & Editors



Hybrid Threats and Hybrid Warfare Reference Curriculum Writing Team Workshop, Berlin, June 2022.



Hybrid Threats and Hybrid Warfare Reference Curriculum Writing Team Workshop, Garmisch-Partenkirchen, February 2022.



## Table of Contents

I. Aim of this Document.....	8
II. Hybrid Threats and Hybrid Warfare.....	8
III. Structure of this Curriculum.....	8
IV. Using this Curriculum.....	9
V. Table of Contents.....	10
Theme 1 – Hybrid War and Hybrid Threats: Background, Definitions, and Debates.....	13
T1-B1: Origins of the Terminology – Hybrid Threats.....	15
T1-B2: Origins of the Terminology – Hybrid Warfare.....	16
T1-B3: Moving Forward – What’s New?.....	18
Theme 2 – Threat Vectors: Domain-related Means and Methods of Exercising Hybrid Threats and Hybrid Warfare.....	21
T2-B1: Information Vectors.....	23
T2-B2: New Technologies as Catalysts for Hybrid Action.....	25
T2-B3: Creating and Exploiting Political, Social, and Cultural Divisions.....	26
T2-B4: Diplomatic Tools.....	28
T2-B5: Economic and Financial Manipulation.....	30
T2-B6: Military Vectors.....	31
T2-B7: Proxy Forces.....	33
T2-B8: Organized Crime.....	34
T2-B9: Lawfare.....	36
T2-B10: Putting It All Together.....	37
Theme 3 – Actors: From Great Powers and Small States to Nonstate and Proxy Actors.....	41
T3-B1: The United States.....	43
T3-B2: China.....	44
T3-B3: Russia.....	47
T3-B4: Regional Powers.....	49
T3-B5: Small States.....	50
T3-B6: Nonstate Actors – NGOs and Cities.....	51
T3-B7: Criminal Networks, Mercenaries, Corporations, and Other Proxy Actors.....	52
T3-B8: Multinational Organizations – EU, NATO, and UN.....	54
Theme 4 – Countering Hybrid Warfare and Hybrid Threats.....	59
T4-B1: Frameworks and Strategies to Counter Hybrid Threats.....	61
T4-B2: The Role of the Military in Response to Hybrid Threats and Hybrid Warfare.....	62
T4-B3: Nonmilitary Approaches and Means for Countering Hybrid Threats.....	64
T4-B4: Information Collection, Analysis, and Sharing.....	65
T4-B5: Coordination and Collaboration in Countering Hybrid Threats.....	67
T4-B6: Scenarios, Wargaming, and Table-Top Exercises (TTX).....	68
T4-B7: Resilience to Hybrid Threats.....	69
T4-B8: Recommended Practices from NATO and EU.....	70
Primary Authors, editors and project leads:.....	72
Discussion Group Leaders & Chief contributors.....	72
Contributors.....	72

# Hybrid Threats and Hybrid Warfare Reference Curriculum

*To win one hundred victories in one hundred battles is not the acme of skill. To subdue the enemy without fighting is the acme of skill.*

- Sun Tzu, The Art of War

## I. AIM OF THIS DOCUMENT

The purpose of the reference curriculum is to provide the reader with a brief, authoritative and reasonably comprehensive, though not exhaustive, guide to addressing the issues of Hybrid Warfare and Hybrid Threats within their various educational venues. This reference curriculum (RC) aims to be authoritative in representing the consensus views of a number of scholars from a representative number of partner nations, and comprehensive to the extent that it seeks to highlight a range of key facets and approaches to these complex subjects. The final document is prescriptive only in highlighting certain agreed elements, issues, and themes. At the minimum it can serve as a tour d'horizon regarding these subjects. The target audience of the reference curriculum is the membership of the PfP Consortium. Ultimately, every nation will have to select from the range of materials offered here and invest in developing their own point of view and approach as appropriate for their geopolitical and strategic needs. In a generalized sense, the themes explored herein should induce readers to consider the rise of Hybrid Warfare and seeming proliferation of Hybrid Threats, and what these mean for their national policies/capabilities at the strategic, operational, and tactical levels and what needs to be incorporated into their various courses from the ab initio through to their higher defence colleges. At the least this document offers guidance in identifying areas that warrant attention and recommends a number of key sources and approaches to these emerging security challenges.

## II. HYBRID THREATS AND HYBRID WARFARE

As the title indicates this reference curriculum addresses both the concept of hybrid warfare and hybrid threats. These terms are not synonymous, but they are related. Both emerged into common parlance over the past decade. Both phrases attempt to affix a label to a number

of related and emergent phenomena in the international security environment. These phrases are not unique to that effort. Concepts like Grey Area threats, Grey Zone or Grey Area Warfare, 'compound' warfare, information warfare, and information operations, unconventional and irregular warfare, cognitive warfare, 'liminal warfare', among others, all compete in this crowded ontological space. Each reflect efforts to find a pithy term or phrase to articulate and encapsulate a series of disparate but interrelated activities seen internationally that aim to challenge the international security status quo through undermining the public will, institutions, actors, and states primarily in aid of some political or military objective by a malign external state actor to the verge of open warfare or across that threshold as supplements to more active military activities. Few of these phrases are recognized as part of official military doctrine but many have entered the common lexicon of the security and defence communities. The range of potential areas of concern or engagement is broad indeed and a number of activities that fall within these concepts may not traditionally be regarded as activities or areas that the armed forces of the western alliance would normally concern themselves. A more complete etymology of the concepts of hybrid war and hybrid threats is provided in the first section of this course.

## III. STRUCTURE OF THIS CURRICULUM

As previous reference curriculum documents have stated, a 'curriculum' is a specific learning programme; however, it may be used to inform a range of courses, or incorporated in part into other courses, according to the needs of those who may use it. This document describes a possible pattern for teaching, learning outcomes and assessment materials for a general course of study. It is in that sense a roadmap that can be followed in whole or in part. Like any map, it is crafted with a level of abstraction that requires interpretation to follow but provides a solid overview of many routes and contours one could follow. As well, the majority of sources referenced are available in English but national need and local requirements suggest many of those who adopt the curriculum will seek sources available in other languages.

Typically, a generic curriculum results in a nested structure, with many subtopics and issues nested within a broader framework. These many nested parts are connected to broader objectives of the full programme of study laid out below; nevertheless, users may choose only portions of this outline to follow and may expand or contract the degree of attention they pay any of the many subjects and issues contained herein according to a multitude of factors, ranging from the student audience they will address to the consideration of time available to expose, explore and engage in critical discussion of these issues. That is all to say while this reference curriculum constitutes a logical whole it does not have to be adopted in totality and course designers may draw upon it as they need in developing their own bespoke programmes of study. Indeed, we will have more than succeeded if this reference curriculum only influences faculty in their choices.

In keeping with the structures adopted in other PfPC reference curricula, this document has grouped the broad discussion into four major theme areas. Each theme area contains recommended blocks for discreet attention. These divisions are designated Themes (T) and Blocks (B) as reflected in the table of contents (see below).

The four themes of this curriculum are as follows:

**Theme 1:** Hybrid War and Hybrid Threats—Foundations, Definitions and Debates

**Theme 2:** Threat Vectors—Means of Exercising Hybrid Threats and Hybrid Warfare

**Theme 3:** Actors: Great Power Competition—Small States—Non-State and Proxy actors

**Theme 4:** Countering Hybrid Warfare and Hybrid Threats

Each theme is described in detail elsewhere in this document but each has broad though specific areas and issues to address.

Subsumed under each theme are distinct subjects and discussions. Each subject is explored in the basic block, which itself may have sub-components, and there are recommended lectures, presentation topics, demonstrations, or similar activities. Since this reference curriculum will require local adaptation, we have not suggested detailed lectures as that level of detail will be contingent on institutional needs. Individual blocks collectively inform each theme area and suggest learning

objectives and outcomes to be achieved; these in turn are connected to the wider objectives of the theme areas. In keeping with the complexity of the subject matter and the interrelationships, aside from the foundational elements, these themes are not to be considered hierarchical. A knowledge ecology approach may prove to be the most productive for the course designer.

## IV. USING THIS CURRICULUM

This RC makes a number of implicit assumptions.

First, all the material identified herein is non-classified and openly available sources only have been utilized or referenced. Institutions adopting this outline should consider how and where they may choose to introduce more sensitive materials and discussions—to certain staff college's courses such sources may be timelier or of greater national relevance.

Second, it is assumed that institutions that seek to utilise this reference curriculum will devote appropriate time and resources to interpreting for their own needs and draw upon subject matter experts (SMEs) and other to translate the broad design into useful and focused learning elements that address their national needs, draw upon local expertise as much as possible, and detail appropriate concepts for the target student body. In developing specific courses local course designers will have to consider time and resources available, and prioritize the learning outcomes appropriate to their student population, regardless of their rank or background.

Third, many issues raised through this reference curriculum could warrant much further discussion than they receive herein. For instance, there is vast and developing literature on Information Operations on which we only touch. We point to a number of ways such topics might be explored more fully but make no claim to exhaustiveness.

Finally, we reiterate that this reference curriculum is not a single or proposed course structure—rather it is a guide for course designers who may be asked to prepare various courses and for various audiences. This document is best considered a key reference providing in broad outline the issues and topics across the spectrum of what are considered hybrid warfare and hybrid threats. It may guide the writing of courses for senior national security personnel, senior military officers and various levels of staff colleges and NCO general courses. The three ele-



ments of greatest concern when utilizing this RC as a guide when designing any single course will be the aim and purpose of the course; the nature of the student body; and, the time and resources that can be dedicated to the course. Those elements should guide the level of detail and forms of learner engagement chosen.

## V. TABLE OF CONTENTS

**Theme 1:** Hybrid War and Hybrid Threats—Foundations, Definitions and Debates

**Theme 2:** Threat Vectors—Means of Exercising Hybrid Threats and Hybrid Warfare

**Theme 3:** Actors: Great Power Competition—Small States—Non-State and Proxy actors

**Theme 4:** Countering Hybrid Warfare and Hybrid Threats



Hybrid Threats and Hybrid Warfare Reference Curriculum Writing Team Workshop, Garmisch-Partenkirchen, February 2022.



Hybrid Threats and Hybrid Warfare Reference Curriculum Writing Team Workshop, Garmisch-Partenkirchen, February 2022.







## Theme 1 – Hybrid War and Hybrid Threats: Background, Definitions, and Debates

### Goal

The goal of this theme is to examine the origins of the terms “hybrid warfare and hybrid threats,” to identify their key features and distinctions, and to explore the debates surrounding the term’s utility and applicability. No single agreed definition exists for either concept, and readers should note that a range of differing definitions and interpretations of these terms are in use.

### Description

The 2014 Russian invasion of Ukraine led to the illegal annexation of the Crimea and the establishment of two breakaway provinces in the Donbas and Luhansk territories of Ukraine. Russia’s subtle—and at first concealed—political and military efforts to foment unrest, generate internal dissent, manipulate political factions, and sow confusion in Ukraine blocked local and international awareness of the risks and threat to Ukraine and allowed Russia to present the world with a fait accompli occupation and dismemberment of the state. The fact Russian troops had disguised their national identities and directly supported insurrectionary forces in the Donbas and Luhansk galvanized attention across western Europe and pushed NATO to scrutinize this type of activity.

After Russia’s 2014 invasion, NATO Heads of State issued a communique that included the terms hybrid threat and hybrid warfare. The first reference combined the terms: “We will ensure that NATO is able to effectively address the specific challenges posed by hybrid warfare threats (emphasis added), where a wide range of overt and covert military, paramilitary, and civilian measures are employed in a highly integrated design.” [Official Communique Wales Summit Declaration, 5 Sept. 2014, para 13.] Further references used threat and warfare interchangeably.

Since the Summit, efforts have been made to address each concept separately. In general, it is broadly recognized that conflict is not just armed violence; it may also include tactics like psychological manipulation, economic exploitation, and the use of graft, subversion, and other means to deepen social divides—all of which are features of hybrid warfare and hybrid threats. By providing a brief survey of these developments, this theme serves as a foundation for those that follow. It

provides an opportunity to examine the origins of the concepts of hybrid threats and hybrid warfare to provide a solid outline or general understanding of the terms.

### Learning Outcomes

Students will be able to:

- 1) Speak about the origins of both hybrid threats and hybrid warfare and articulate the distinctions between them.
- 2) Frame such concepts as they relate to wider strategic military theories on the indirect approach and attacks against the national will.
- 3) Reflect on the fluidity and adaptability of the concepts of hybrid threats and hybrid warfare.
- 4) Identify common elements between the concepts of hybrid threats and hybrid warfare.
- 5) Articulate some of the interdisciplinary challenges posed by hybrid threats and hybrid warfare.

### Suggested References

Discussion may include the distinctions among formal warfare, legally declared states of war, and violent or malevolent activity by state and nonstate actors that fall short of meeting the legal criteria to be called warfare. Some general sources are recommended below.

For a focused discussion on the origins and evolution of the terms hybrid threats and hybrid warfare, it is recommended the instructional staff begin with a detailed examination of the following three works:

Ofer Fridman, *Russian Hybrid Warfare. Resurgence and Politicisation*, 2nd ed. (Oxford: Oxford University Press, 2022).

Mark Galeotti, *The Weaponization of Everything*, (New Haven: Yale University Press, 2022).

Bernd Horn, *On Hybrid Warfare*. (CANSOFCOM: Canada, 2016).

General Discussion of Warfare in Classical Theory:

First chapter *On War*, Clausewitz, various editions.

Sun Tzu *Art of War* (any edition).

Edward Luttwak, *Strategy The Logic of War and Peace* (Boston: Harvard University Press, 2002).

Colin S. Grey, *Modern Strategy* (Oxford: Oxford University Press, 1999).

General Discussion of Hybrid Threats and Hybrid Warfare:

Jan Joel Andersson and Thierry Tardy, “Hybrid: What’s in a Name?” European Union Institute for Security Studies (EUISS), 2015. <https://doi.org/DOI.10.2815/422877>.  
Sascha-Dominik Bachmann, “Hybrid Wars: The 21st Century’s New Threat To Global Peace and Security,” and H. Gunneriusson and R. Ottis. “Cyberspace From the Hybrid Threat Perspective.” *Journal of Information Warfare* 12, no. 3 (2013), 67–77.

Christopher C. Chivvis, “Understanding Russian “Hybrid Warfare” and What Can Be Done About It?” (Santa Monica, CA, RAND Corporation, 2017), [https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT468/RAND\\_CT468.pdf](https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT468/RAND_CT468.pdf).

Brian P. Fleming, “Hybrid Threat Concept: Contemporary War, Military Planning and the Advent of Unrestricted Operational Art,” (monograph, School of Advanced Military Studies, Army Command and General Staff College, Fort Leavenworth, KS, May 19, 2011) <https://apps.dtic.mil/sti/citations/ADA545789>.

Colin S. Gray, “Categorical Confusion? The Strategic Implications of Recognizing Challenges Either as Irregular or Traditional,” (monograph, Strategic Studies Institute, Army War College, Carlisle Barracks, PA, February 1, 2012) <https://apps.dtic.mil/sti/citations/ADA559162>.

Frank G. Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars* (Arlington: Potomac Institute for Policy Studies, 2007).

Petri Huovinen, “Hybrid Warfare—Just a Twist of Compound Warfare?: Views on Warfare From the United States Armed Forces Perspective,” National Defence University [Finland] Department of Military History, April 2011.

Ilmari Kähkö, “The Evolution of Hybrid Warfare: Implications for Strategy and the Military Profession,” *The US Army War College Quarterly: Parameters* 51, no. 3 (25 August 2021).

Salamah Magnuson, Morgan Keay, and Kimberly Metcalf, “Countering Hybrid Warfare: Mapping Social Contacts To Reinforce Social Resiliency in Estonia and Beyond,” *Texas National Security Review*, Spring 2022, <https://tnsr.org/2022/01/countering-hybrid-warfare-mapping-social-contracts-to-reinforce-societal-resiliency-in-estonia-and-beyond/>.

John J. McCuen, “Hybrid Wars,” *Military Review*, April 2008, 107–113, [https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview\\_20080430\\_art017.pdf](https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20080430_art017.pdf).

Timothy McCulloh and Richard Johnson, “Hybrid Warfare,” Joint Special Operations University, MacDill Air Force Base FL, August 1, 2013, <https://apps.dtic.mil/sti/citations/ADA591803>.

Seth B. Neville, “Russia and Hybrid Warfare: Identifying Critical Elements in Successful Applications of Hybrid Tactics,” (Monterey, CA: Naval Postgraduate School, December 2015).

Erik Reichborn-Kjennerud and Patrick Cullen, “What Is Hybrid Warfare?,” Norwegian Institute of International Affairs (NUPI), 2016. <https://www.jstor.org/stable/resrep07978>.

Donald Stoker and Craig Whiteside, “Blurred Lines: Gray Zone Conflict and Hybrid War—Two Failures of American Strategic Thinking,” [U.S.] *Naval War College Review*, 37 no.1 (Winter 2020).

Rob De Wijk, “Hybrid Conflict and the Changing Nature of Actors,” in *The Oxford Handbook of War*, eds. Julian Lindley-French and Yves Boyer (Oxford: Oxford University Press, 2012) 358–372.

## T1-B1: Origins of the Terminology – Hybrid Threats

### Description

This block examines the definition of hybrid threats and illustrates the genesis of the concept.

Rather than adopting the terms war or warfare, various reasons—some political, others prosaic or legal—endorse focusing on threats. The terms may be seen as excessively militarizing the discussion, and a good deal of literature suggests that using the term securitization—a phenomenon where many interests serve to turn political issues into military issues—is a real concern in the defence and security academic community. The concept of war in the international system is defined by a legal framework and statutes. National definitions in law or practice may differ. Traditional military forces in many states do not play an internal security role, but it is precisely to internal security measures that many states must turn to address hybrid risk threat vectors. Hybrid threats, then, speak largely to activities short of formal warfare, but that does not mean such threats are not also present during formal war.

Hybrid threat refers to potential overt and covert military and nonmilitary actions that a state or nonstate actor might take to undermine a targeted society and achieve their political goals. These actions go beyond the normal interaction of states, without necessarily seeking a warlike aim. Not all hybrid threats can be clearly classified as military problems. Theme 2 will address the wide range of activities associated with hybrid threats in more detail; discussion here should focus on the general concept as developed in a sampling of the literature indicated below.

### Learning Outcomes

Students will be able to:

- 1) Articulate the blurred character and the fluidity of the phenomenon of contemporary hybrid threats.
- 2) Understand the origins of the term hybrid threats.

### Issues for Potential Modules and Approaches To Consider

Course designers should engage local subject matter experts to decide the appropriate level of detail needed for their national audience. Some material is best developed after considering the lived national experience and

roles and missions of the state's national security apparatus, because many activities associated with hybrid threats may not be the primary focus of their national military forces, but may fall to other national security actors—domestic or international intelligence agencies, police, or other government agencies. Such divisions should be mapped as part of the course development process, and where possible, experts from those other agencies should be consulted, if not directly involved in providing relevant materials.

Conceptualize hybrid threats and provide an overview of potential hybrid threat vectors on a broad variety of domains.

Address European Union and NATO perspectives.

### Learning Method/Assessment

Learning methods may include lectures, guest speakers, video case studies, role playing, blogging, case studies, practical exercises, readings, research, article reviews, small group exercises, and reflective journaling.

### References

In addition to the References provided see:

P. Cullen, et al., *The Landscape of Hybrid Threats: A Conceptual Model*, G. Giannopoulos, H. Smith, M. Theodoridou, eds. (Luxembourg, European Commission, Hybrid CoE, 2021) [https://publications.jrc.ec.europa.eu/repository/bitstream/JRC123305/conceptual\\_framework-reference-version-shortened-good\\_cover\\_-\\_publication\\_office\\_1.pdf](https://publications.jrc.ec.europa.eu/repository/bitstream/JRC123305/conceptual_framework-reference-version-shortened-good_cover_-_publication_office_1.pdf).

Aleks Nesic and Arnel P. David, "Operationalizing the Science of the Human Domain in Great Power Competition for Special Operations Forces," *Small Wars Journal*, April 14, 2019, <https://smallwarsjournal.com/jrnl/art/operationalizing-science-human-domain-great-power-competition-special-operations-forces>.



## T1-B2: Origins of the Terminology – Hybrid Warfare

### Description

This block will provide participants with an understanding of the origins and contemporary character of hybrid warfare. Hybrid warfare may incorporate regular and irregular military capabilities with activities across the full spectrum of diplomatic, economic, informational, and social manipulation in the furtherance of the adversary's goals, keeping below the level or threshold of conventional war. Such activity may be both covert and overt.

The term hybrid warfare began appearing more broadly in security literature about 2005. Originally it referred to confronting unconventional forces, such as the Taliban in Afghanistan or local insurgents, such as those in Iraq. However, the term has become associated with the challenges posed by coordinated, novel, and not purely military malign actions undertaken by state actors. These actors have incorporated several nontraditional or nonconventional means to undercut national will, sow discord, confuse political actions and actors, and undermine national authority, political legitimacy, and the freedom to maneuver among target nations or populations.

The term hybrid warfare is still problematic because of the inherent ambiguity in its use. It is a term that lacks precision in the same manner that the term terrorism does. Tarik Somaz identifies five related, but distinct, uses of the term hybrid warfare:

- 1) The employment of synergistic fusion of conventional weapons, irregular tactics, terrorism, and criminal activities in the same battlespace.
- 2) The combined use of regular and irregular forces under a unified direction.
- 3) The use of various military and nonmilitary means to menace an enemy.
- 4) Subthreshold activities involving any mix of violent and nonviolent means.
- 5) A way to achieve political goals by using nonviolent subversive activities.

[Tarik Solmaz, “‘Hybrid Warfare:’ One Term, Many Meanings,” *Small Wars Journal*, February 25, 2022.]

We acknowledge room for criticism of how we use the terms hybrid threats and hybrid warfare because of the

continuing ambiguity over their exact meaning. We can argue the terms are in sufficiently wide use that they are unlikely to disappear, and they do seem to speak to “a novel yet distinct form of warfare conducted by states” and some nonstate actors. [see Eric Reichborn-Kjennerud and Patrick Cullen, “What Is Hybrid Warfare,” Policy Brief 1/16 Norwegian Institute of International Affairs, (Oslo) 2016].

We can look to the meaning of the term hybrid to help clarify meaning. Although originally a noun, hybrid is also now used as an adjective. As a noun, hybrid refers to something composed of two different elements not normally combined, which in nature would be a new species. As an adjective, hybrid denotes something being of mixed character composed of different elements. In either form, the term refers to an unusual mating or joining together. Given that sense, we can say that with hybrid threats and hybrid warfare, the individual parts may not be new or novel. However, the combination of actions/activities is novel—although perhaps not unique—to traditional military conceptions of threats/aggression and to civil authorities whose sensibilities of what constitutes a national security threat/concern will be challenged to expand.

Although considerable debate exists in the academic literature over the veracity or utility of the term hybrid warfare, its wide use clearly suggests that a concept of modern war that only envisions a conventional military threat is outmoded. Our working definition of hybrid warfare is as follows:

*Hybrid warfare is the creative use of hard, soft, and smart power by malign state or nonstate actors to achieve war-like objectives and political goals. Malign acts include a broad spectrum of military and nonmilitary instruments of coercive power beyond the conventionally conceived multidomain battlespace. Hybrid warfare encompasses politics, diplomacy, information, the economy, technology, the military and society, as well as dimensions like culture, psychology, legitimacy and morale. The coordinated performance of these malign acts occur both overtly and covertly in the ambiguous grey zones of blurred interfaces: between war and peace, friend and foe, internal and external relations, civil and military, and state and nonstate actors, as well as in fields of responsibilities generally below the threshold of war or as an accompaniment to more regular armed conflict.*

## Learning Outcomes

The students will be able to:

- 6) Understand the origins and historical evolution of the concept of hybrid warfare.
- 7) Understand the employment of instruments of national power in the full spectrum of conflict.
- 8) Understand the range of activities associated with hybrid warfare.
- 9) Analyze recent cases of hybrid warfare.

## Issues for Potential Modules and Approaches to Consider

The conceptualization of hybrid warfare and respective working definitions.

Historical and current case studies to exemplify the development of theory based on empirical evidence.

Utilizing the interdisciplinary approach to studying hybrid warfare.

Including disciplinary perspectives: anthropology, economics political science, psychology, and sociology.

Units of Analysis (individual, subnational (urban/rural/tribal/ethnic) national, regional and global)

The combination of military and nonmilitary vectors in a hybrid confrontation.

## Learning Method/Assessment

Learning methods may include lectures, guest speakers, video case studies, role playing, blogging, case studies, practical exercises, readings, research, article reviews, small group exercises, and reflective journaling.

## References

\*Much of the discussion above is drawn from Sean Monaghan, "Information Note, MCDC Countering Hybrid Warfare Project. Countering Hybrid Warfare: Conceptual foundations and Implications for Defence Forces," March 2019.

Frank Hoffman, "Further Thoughts on Hybrid Threats," Small Wars Journal, March 3, 2009, <http://smallwarsjournal.com/blog/2009/03/further0thoughts-on-hybrid-thr>.

Ilmari Kähkö, "The Evolution of Hybrid Warfare: Implications for Strategy and the Military Profession," U.S. Army War College, Parameters 51, no. 3 (2021), <https://press.armywarcollege.edu/parameters/vol51/iss3/11>.

James Mattis and Frank Hoffman, "Future Warfare: The Rise of Hybrid Wars," U.S. Naval Institute Proceedings, vol. 131/11/1233, [www.usni.org/magazines/proceedings/2005/november](http://www.usni.org/magazines/proceedings/2005/november).

Sean Monaghan, "Countering Hybrid Warfare: So What for the Future Joint Force?," U.S. National Defense University Press, PRISM 8, no.2, October 2019, [https://ndupress.ndu.edu/Portals/68/Documents/prism/prism\\_8-2/PRISM\\_8-2\\_Monaghan.pdf](https://ndupress.ndu.edu/Portals/68/Documents/prism/prism_8-2/PRISM_8-2_Monaghan.pdf).

Eric Reichborn-Kjennerud and Patrick Cullen, "What is Hybrid Warfare?" Norwegian Institute of International Affairs (NUPI) Policy Brief 1/2016.

Johann Schmid, "Introduction to Hybrid Warfare—A Framework for Comprehensive Analysis," in Hybrid Warfare Future and Technologies, Edition ZfAS, ed. Ralph Thiele (Wiesbaden, Springer VS, 2021), 11-32.

Johann Schmid, "Hybrid Warfare in Vietnam—How To Win a War Despite Military Defeat," in ISPAIM—Monitor Strategic 2—4/2020, Feb 2021, 54-67. <https://www.hybridcoe.fi/contributions/hybrid-warfare-in-vietnam-how-to-win-a-war-dispite-military-defeat/>.

Johann Schmid, "Hybrid Warfare on the Ukrainian Battlefield: Developing Theory Based on Empirical Evidence," Sciendo: Journal on Baltic Security, 5(1) August 2019, 5-15, <http://www.degruyter.com/view/j/jobs.2019.5.issue-1/jobs-2019-0001/jobs-2019-0001.xml>.

Johann Schmid, "Hybrid Warfare—Operating on Multidomain Battlefields," NATO Command and Control Centre of Excellence (NATO C2COE), Seminar 2020 Multi Domain Operations (Sept/Nov 2020), <https://c2coe.org/2020/09/09/seminar-read-ahead-hybrid-warfare-operating-on-multi-domain-battlefields/>.

James K. Wither, "Making Sense of Hybrid Warfare," Connections 15, no. 2 (2016): 73–87. <http://www.jstor.org/stable/26326441>.

## T1-B3: Moving Forward – What’s New?

### Description

It may be argued that the forms of hybrid threats and the means of hybrid warfare are not new. However, the range of possible actions that a malign power or transnational violent extremist organization could use in pursuit of their goals poses challenges to many national defence and national security policies and practices. Many states have organized their defences to address a binary model of either war or peace. As such, they are not appropriately structured to deal with challenges across the ‘gray zone’ between war and peace. Indeed, many states have laws, structures, and practices to minimize security information sharing, and lack national coordination of efforts to address such persistent challenges—even if they are recognized as threats.

This block addresses the challenge of transitioning legacy structures, policies, and procedures to ones that more fully address the active multi-faceted challenges of the age of hybrid threats and hybrid warfare. Discussion will move from general considerations to specific national policies and organizational roles and responsibilities.

If awareness of a problem is the first means of addressing it, the discussion here and that follows aims to develop and enhance awareness of both forms of Hybrid Threats and Hybrid Warfare so that prepared states can contemplate how to best acknowledge, identify, deter, mitigate or defend against such challenges in keeping with national and international legal norms and national values and organizations—only some of which are strictly military.

### Learning Outcomes

Participants in the course will be able to

- 1) Articulate all features that allow an external actor to use the full spectrum of the instruments of national power to develop, engage, exploit, and influence state populations, policies, and actions.
- 2) understand that an interdisciplinary approach is key to understand the full spectrum of hybrid threats and hybrid warfare.
- 3) Articulate and understand the contemporary character of hybrid threats and warfare

### Issues for potential Modules and Approaches To Consider

It is recommended that local subject matter experts identify key domestic organizations across the spectrum of issues and engage them in developing resources. These resources must be appropriate for the participant population addressing national policies and practices for identifying such threats and responding to them.

### Learning Method/Assessment

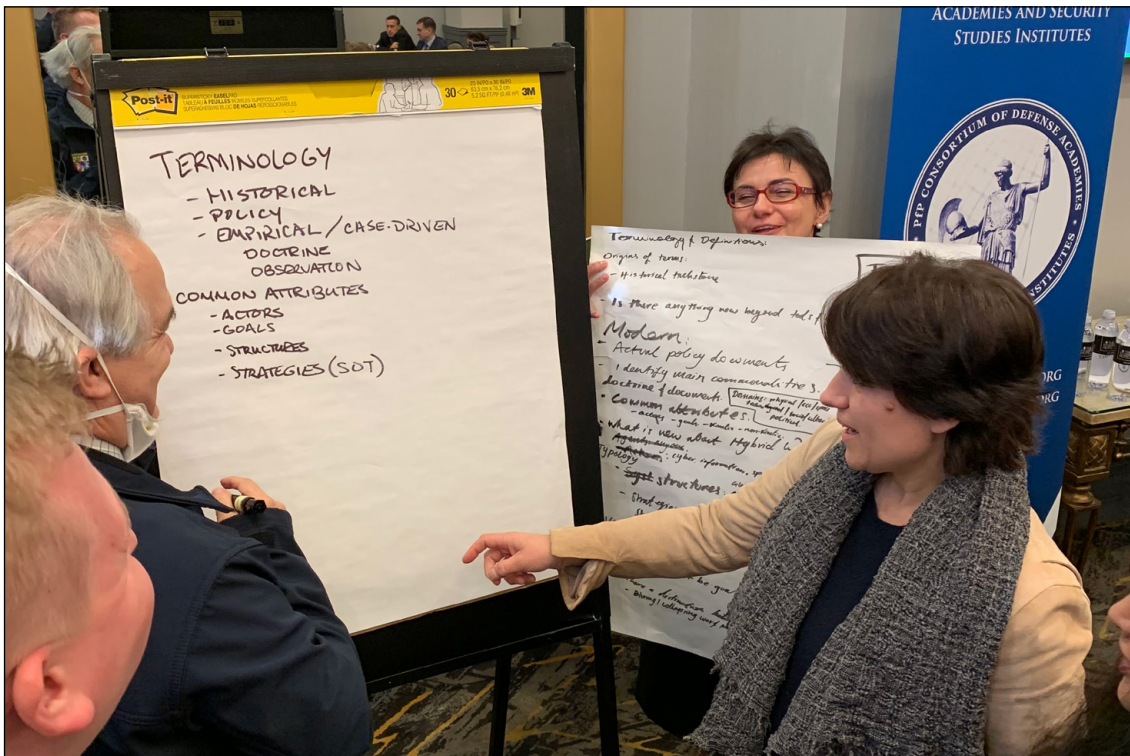
The course may address this block through a challenge and response model for simulation and discussion.

Students should be able to articulate challenges to security intelligence sharing within existing organizations nationally and multinationally.

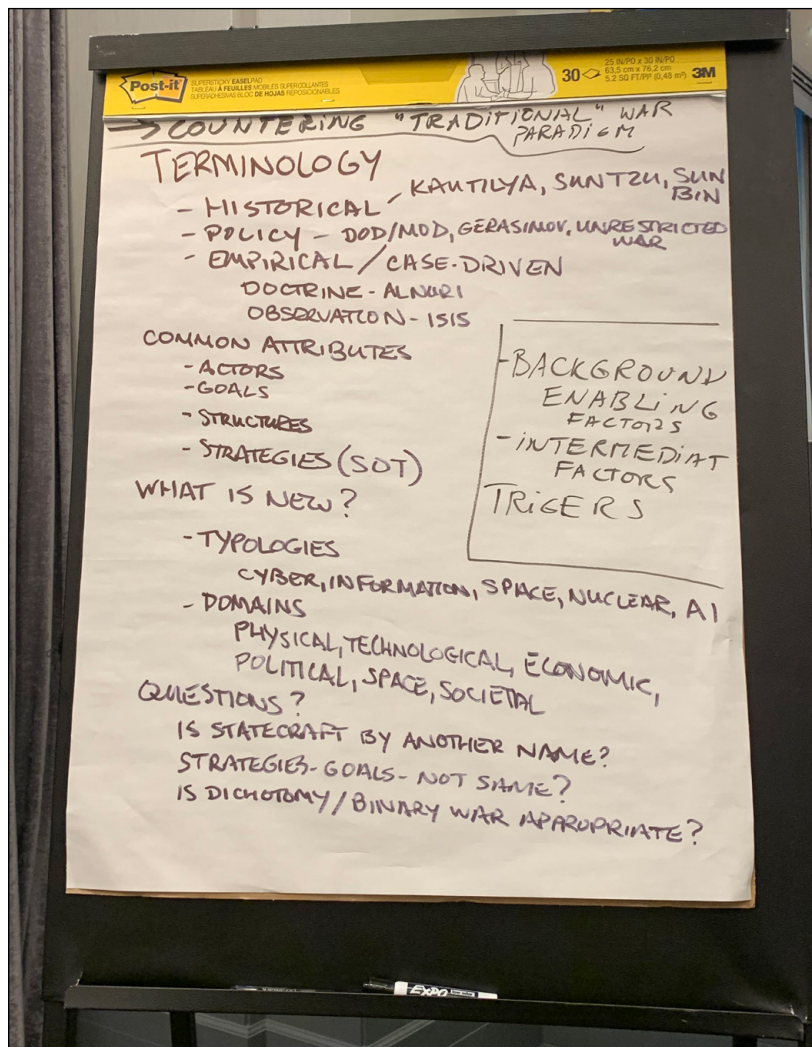
### References

- Arsalan Bilal, “Hybrid Warfare–New Threats, Complexity, and ‘Trust’ as the Antidote,” NATO Review, November 30, 2021, <https://www.nato.int/docu/review/articles/2021/11/30/hybrid-warfare-new-threats-complexity-and-trust-as-the-antidote/index.html>.
- Alex Deep, “Hybrid War: Old Concept, New Techniques,” Small Wars Journal, March 2, 2015. [www.smallwarsjournal.com/jrnl/art/hybrid-war-old-concept-new-techniques](http://www.smallwarsjournal.com/jrnl/art/hybrid-war-old-concept-new-techniques).
- Tarik Solmaz, ““Hybrid Warfare”: One Term, Many Meanings,” Small Wars Journal, February 25, 2022. [www.smallwarsjournal.com/art/hybrid-warfare-one-term-many-meanings](http://www.smallwarsjournal.com/art/hybrid-warfare-one-term-many-meanings).





Hybrid Threats and Hybrid Warfare Reference Curriculum Writing Team Workshop, Garmisch-Partenkirchen, February 2022.



Hybrid Threats and Hybrid Warfare Reference Curriculum Writing Team Workshop, Garmisch-Partenkirchen, February 2022.





**Theme 2 – Threat Vectors: Domain-related Means and Methods of Exercising Hybrid Threats and Hybrid Warfare**

**Goal**

The Goal of this theme is to explore a number of hybrid threat, risk, attack, and warfare vectors by which an adversary can achieve its Goals in different domains. Vectors in this context should be understood as domain-related lines of operation or courses of action (COAs). This theme presents an overview of vectors commonly ascribed to hybrid threats/hybrid warfare. Different vectors may be employed simultaneously within multidomain hybrid warfare campaigns. These vectors may be invisible during the potentially long-lasting, preparatory phase of hybrid campaigns. Such campaigns could include various ways and means, and horizontal and vertical escalation to include the use of conventional force and nuclear options.

**Description**

The term “vector” refers to domain-related actions or operations — that is, actions and operations that target domains such as cultural, societal, religious, political, diplomatic, information, military, economic, financial, intelligence, and law enforcement. The vectors are the means and methods used by adversaries to achieve their

objectives and Goals. As the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) demonstrates in the graphic below, hybrid threat actors undertake actions across a wide range of non-traditional fronts. Moreover, threat vectors could be covert or overt influence operations aimed to sow confusion or division, recruit internal support, erode national will, co-opt elites, and widen social fissures. A plurality of vectors used to advance hybrid warfare operations is explored in this lesson. In particular discussion below, table 1, addresses the following topics:

Informational vectors
Technological
Social, political and cultural
Diplomatic
Economic / financial
Military
Proxy forces
Organized Crime
Lawfare

Table 1: Vectors for Hybrid Threats and Hybrid Warfare  
Note: Traditional military domains (land, air, sea, cyber, and space) should also be considered.

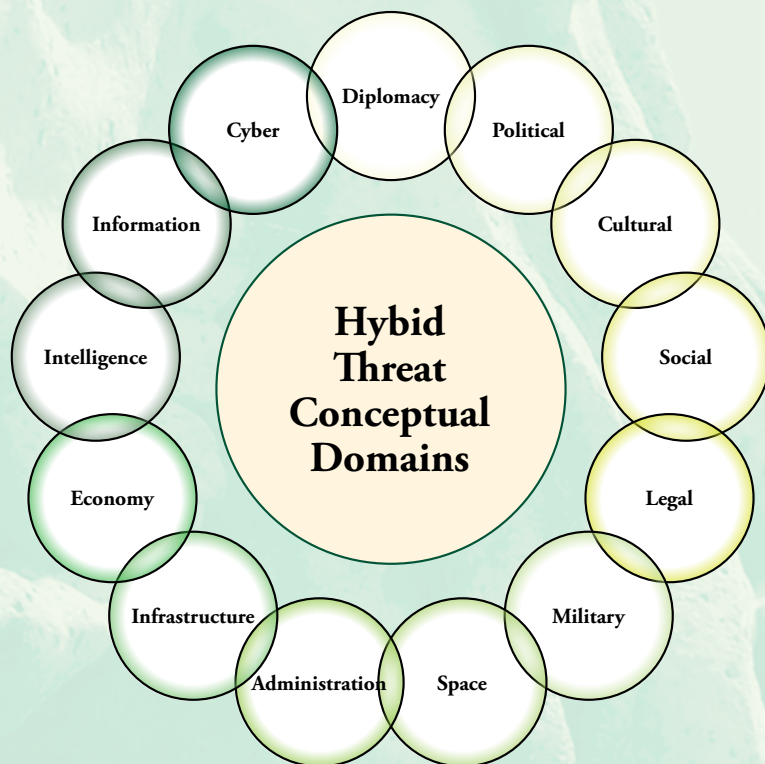


Figure 1. Hybrid threat conceptual domains from The Landscape of Hybrid Threats (Finland: Hybrid CoE, 2021).



## Background

Examination of hybrid threat vectors is critical because of the increased complexity of their means and methods and the proliferation of state and nonstate actors involved in their use. Moreover, the blurring of military and nonmilitary actions can impact multiple domains and have a cumulative effect in undermining societal stability and cohesion. Gaps in a state's understanding of the significance and effects of hybrid means can undermine its ability to be resilient and defend itself — pointing to the need for clear conceptual frameworks to better assist in responses to hybrid threats and warfare. Although hybrid threat activities are not new, modern information and communications technologies are enabling increased access to new channels of influence. As a result, state and nonstate actors have more attack surfaces against which to conduct their operations.

## Learning Outcomes

Students will be able to:

- 1) Describe hybrid threat vectors and how they are used as a means of exercising hybrid warfare.
- 2) Identify methods used to conduct hybrid warfare.
- 3) Outline domain-specific and multi-domain vulnerabilities open to exploitation by hybrid activities.

## Suggested References

Arsalan Bilal, «Hybrid Warfare – New Threats, Complexity, and ‘Trust’ as the Antidote,» NATO Review, November 30, 2021, <https://www.nato.int/docu/review/articles/2021/11/30/hybrid-warfare-new-threats-complexity-and-trust-as-the-antidote/index.html>.

Mason Clark, Russian Hybrid Warfare, Institute for the Study of War, September 2020, <https://www.understandingwar.org/sites/default/files/Russian%20Hybrid%20Warfare%20ISW%20Report%202020.pdf>.

Georgios Giannopoulos, Hanna Smith, and Marianthi Theocharidou, eds., The Landscape of Hybrid Threats: A Conceptual Model, European Commission and Hybrid CoE, 2021, <https://www.hybridcoe.fi/publications/the-landscape-of-hybrid-threats-a-conceptual-model/>.

NATO's Response to Hybrid Threats, North Atlantic Treaty Organization, last modified February 10, 2023, [https://www.nato.int/cps/en/natohq/topics\\_156338.htm](https://www.nato.int/cps/en/natohq/topics_156338.htm).

«Hybrid Threats as a Concept,» Hybrid CoE, The European Centre of Excellence for Countering Hybrid Threats, accessed September 16, 2022, <https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/>

“EU Policy on Fighting Hybrid Threats,» The NATO Cooperative Cyber Defence Centre of Excellence, accessed September 16, 2022, <https://ccdcoe.org/incyber-articles/eu-policy-on-fighting-hybrid-threats/>.

Janne Jokinen and Magnus Normark, Hybrid Threats from Non-state Actors: A Taxonomy, Hybrid CoE Research Report 6, The European Centre of Excellence for Countering Hybrid Threats, June 2022, <https://www.hybridcoe.fi/wp-content/uploads/2022/05/20220609-Hybrid-CoE-Research-Report-6-Non-state-actors-WEB.pdf>.

Johann Schmid, “Hybrid Warfare in Vietnam – How to Win a War Despite Military Defeat,” ISPAIM–Monitor Strategic, *B.Nr.* 17 (February 12, 2020): 54-67, [https://www.hybridcoe.fi/wp-content/uploads/2021/03/210302\\_HW-in-Vietnam\\_table-of-content.pdf](https://www.hybridcoe.fi/wp-content/uploads/2021/03/210302_HW-in-Vietnam_table-of-content.pdf).

Johann Schmid, “Hybrid Warfare on the Ukrainian Battlefield: Developing Theory Based on Empirical Evidence,” Journal on Baltic Security, 5, no. 1 (2019): 5-15, [https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/resources/docs/BDC\\_1\\_23829230%20-%20Journal%20on%20Baltic%20Security%20Hybrid%20warfare%20on%20the%20Ukrainian%20battlefield\\_%20developing%20theory%20based%20on%20empirical%20evidence.pdf](https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/resources/docs/BDC_1_23829230%20-%20Journal%20on%20Baltic%20Security%20Hybrid%20warfare%20on%20the%20Ukrainian%20battlefield_%20developing%20theory%20based%20on%20empirical%20evidence.pdf).

Johann Schmid, Hybrid Warfare – Operating on Multidomain Battlefields, read-ahead article for 2020 Multi Domain Operations Seminar, NATO C2COE, 2020, <https://c2coe.org/2020/09/09/seminar-read-ahead-hybrid-warfare-operating-on-multi-domain-battlefields/>.

## T2-B1: Information Vectors

### Description

States and societies thrive on information. There is a wide and rich debate on information. Information can inform and be used to shape opinions. Individuals consume information today through traditional media—magazines, newspapers, radio, and television—and social media—blogs, videos, vlogs, and live streaming. Information can be manipulated for specific purposes, and defining these manipulations can help students understand their use. The discussion here will focus on several key issues and definitions, notably:

Disinformation is deliberately created to mislead, harm, or manipulate a person, social group, organization, or country.
Misinformation is false but shared without the intention of causing harm.
Malinformation is based on fact, but used out of context to deliberately mislead, harm, or manipulate.

Table 2: MDM Definitions, CISA, <https://www.cisa.gov/mdm>.

Note: For this section, disinformation and malinformation could be understood as deliberately weaponized information (e.g., propaganda). Disinformation and malinformation are not independent entities, but they overlap and often are not clearly distinguished. A state or nonstate actor can use the confusion caused by both misinformation and malinformation to create disinformation. All three approaches are used in information operations, psychological warfare, and hybrid warfare.

### Background

Weaponized information threatens the democracies of the European Union, NATO, and its partner nations across the world. It creates distrust in national, regional, and global institutions, as well as local and national governments. Weaponized information is a critical component of both hybrid threats and hybrid warfare, and is used by state and nonstate actors to achieve a particular Goal. As a result, we now see the rise of a body of literature on narrative warfare, cognitive warfare, and similar concepts.

Weaponized information may be used by state and nonstate actors to create false narratives. Increasingly, weaponized information is also being used by criminal entities to entice vulnerable people into situations where they face great harm (e.g., trafficking) or to monetize their criminal activities (e.g., fraud). Weaponized information is being used to support hostile state activity, foment political violence and extremism, or enable criminal activity through cyberspace. Malign actors exploit the expectation for accurate information by creating confusion and obscuring the truth.

### Learning Outcomes

Students will be able to:

- 1) Understand that misinformation, disinformation, and malinformation are activities employed in hybrid warfare.
- 2) Analyze how weaponized information is being used, exploited, and executed by malign actors, which is crucial to devising countermeasures.

### Issues for Potential Modules and Approaches to Consider

- The range of actors using weaponized information is broad.
- The concept of weaponized information does not fit neatly into one category.
- Current countermeasures to weaponized information should be considered.
- Identify and understand the resilience mechanisms (in particular, regarding social cohesion) to prevent and counter weaponized information.

### Learning Method / Assessment

Learning methods may include interactive exploration, for example, through lectures, case studies, role playing, blogging, exercises and games, workshops, group discussions, and reflective journaling. Instructors should use all modes of instruction and use real-world examples.



## References

- Michael K. Buckland, "Information as Thing," *Journal of the American Society for Information Science*, 42, no. 5 (June 1991): 351-60, [https://asistdl.onlinelibrary.wiley.com/doi/10.1002/\(SICI\)1097-4571\(199106\)42:5%3C351::AID-ASI5%3E3.0.CO;2-3](https://asistdl.onlinelibrary.wiley.com/doi/10.1002/(SICI)1097-4571(199106)42:5%3C351::AID-ASI5%3E3.0.CO;2-3).
- Nollag Conneely, «The Infodemic of Disinformation: What is the Defence Forces' Role in Mitigating the Threat of Disinformation to National Security in Ireland?» MA thesis, Maynooth University, 2021.
- Sean S. Costigan and Todor Tagarev, "Countering Crime, Hate Speech, and Disinformation in Cyberspace," *Connections: The Quarterly Journal*, 20, no. 2 (2021): 5-8, <https://connections-qj.org/article/countering-crime-hate-speech-and-disinformation-cyberspace>.
- Yuriy Danyk, Tamara Maliarchuk, and Chad Briggs. "Hybrid War: High-tech, Information and Cyber Conflicts," *Connections: The Quarterly Journal*, 16, no. 2 (2017): 5-24, <https://connections-qj.org/article/hybrid-war-high-tech-information-and-cyber-conflicts>.
- Mark Galeotti, *The Weaponisation of Everything: A Field Guide to the New Way of War* (New Haven, CT: Yale University Press, 2022).
- Albert H. Hastorf and Hadley Cantril, "They Saw a Game: A Case Study," *The Journal of Abnormal and Social Psychology*, 49, no. 1 (1954): 129-34.
- Dinos Kerigan-Kyrou, «Protecting Cyberspace: A Hybrid Threat Requires a Hybrid Response,» *An Cosantoir*, 79, no. 4 (May 2019): 18-19, <http://digital.jmpublishing.ie/i/1111057-may-2019/17?token=null>.
- Henry Kissinger, *World Order* (New York: Penguin Press, 2014), especially Chapter 9, "Technology, Equilibrium, and Human Consciousness."
- Merle Maigre, *Cyber Threat Actors: How to Build Resilience to Counter Them*, Hybrid Centre of Excellence, Paper 11, February 2022, <https://www.hybridcoe.fi/wp-content/uploads/2022/02/20220209-Hybrid-CoE-Paper-11-Cyber-threat-actors-WEB.pdf>.
- Johann Schmid, «Challenges of Hybrid Threats/Warfare,» presentation at the CODE Conference 2020, Workshop 5, Munich, Germany, November 11, 2020, <https://www.unibw.de/code/events/code2020-workshops>.
- We're in This Together. Mis-, Dis-, and Malinformation Stops with You, Cybersecurity and Infrastructure Security Agency, accessed October 7, 2022, [https://www.cisa.gov/sites/default/files/publications/election-disinformation-toolkit\\_508\\_0.pdf](https://www.cisa.gov/sites/default/files/publications/election-disinformation-toolkit_508_0.pdf).
- ENISA Threat Landscape Report, European Union Agency for Cybersecurity, October 2021, [www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends](http://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends).
- Mission Report: Special Committee on Foreign Interference in all Democratic Processes in the European Union, including Disinformation, European Parliament, March 29, 2022, [www.europarl.europa.eu/doceo/document/INGE-CR-719939\\_EN.docx](http://www.europarl.europa.eu/doceo/document/INGE-CR-719939_EN.docx).
- "Opening Statement by Foreign Minister Annalena Baerbock at the Conference on Facts vs. Disinformation," Federal Republic of Germany, Federal Foreign Office, May 4, 2022, [www.auswaertiges-amt.de/en/newsroom/news/disinformation-conference-speech/2521260](http://www.auswaertiges-amt.de/en/newsroom/news/disinformation-conference-speech/2521260).

## **T2-B2: New Technologies as Catalysts for Hybrid Action**

### **Description**

This section examines the implications of new technologies and their disruptive potential in a hybrid warfare and threats context. The current technological revolution has transformed the intersection between technology and hybrid warfare/hybrid threats.

### **Background**

Hybrid warfare and threats are an age-old phenomenon, which today is significantly empowered by new technological developments. To prevent, defend against, counter, or outmaneuver hybrid adversaries, leaders and decision-makers must develop a common understanding of new technologies, with emphasis on what enables these new attack vectors. New technologies, with their disruptive potential, have a catalytic effect on hybrid means, methods, tactics, and strategies. Emerging technologies may improve the starting conditions for hybrid action, expand the arsenal of hybrid players, and thus help to increase the reach of their activities as well as their prospects of success. Particularly worrying is that they provide offensive options. However, the technological developments not only offer improved capabilities to understand the threat landscape and counter hybrid attacks, but they also enable adversaries to create new hybrid risk and threat vectors.

Globalization has increased the speed at which new technologies are being developed as well as their accessibility. While investing in new technology may give states a competitive advantage to counter hybrid threats, they may also create vulnerabilities, which may be exploited by malign actors.

Most importantly, new technological trends increasingly turn technology into a “battlespace” for hybrid confrontation. Against this backdrop, technology constitutes an additional domain and a possibility for hybrid actors to horizontally extend the battlespace and create new hybrid risk/attack vectors. The technological domain may even turn into the center of gravity in a hybrid confrontation.

The following technologies are relevant to the evolution of hybrid warfare/threats and respective risk vectors: 5G, additive manufacturing (e.g., 3D printing), arti-

cial intelligence, autonomous systems, biotechnology, nano-biotechnology, cloud computing, communication networks, cyber and electronic warfare, blockchain or distributed ledger, directed energy, extended or virtual reality, hypersonics, Internet of Things, micro-electronics, nano-materials, nuclear modernization, quantum sciences, space, and ubiquitous sensors.

### **Learning Outcomes**

Students will be able to:

- 1) Understand technology as a relevant and dynamic factor in the context of hybrid warfare/threats with two perspectives:
- 2) Technology as a disruptive hybrid risk/attack vector, and
- 3) Technology as a vector to counter hybrid adversaries.
- 4) Appreciate the implications of new technologies and their disruptive potential in a hybrid warfare and threats context.
- 5) Understand the intersection of technology and the hybrid warfare/threat spectrum.

### **Issues for Potential Modules and Approaches to Consider**

- Raising awareness of technology as a relevant and dynamic factor in the context of hybrid warfare/threats based on selected case studies.
- Lecture/discussion: Technology is not only a catalyst for hybrid warfare/threats, but also an enabler of countering hybrid adversaries.
- Deep-dive case studies on the use of selected technologies (for example, the use of drones for hybrid warfare battlefields) to enhance the understanding of hybrid risk/attack vectors.
- Include subject matter experts in technology.

### **Learning Method/Assessment**

Learning methods may include lectures, guest speakers, video case studies, role playing, blogging, case studies, practical exercises, strategic games, workshops, group discussions, readings, research, article reviews, small-group exercises and reflective journaling.

## References

Elsa B. Kania, “Minds at War: China’s Pursuit of Military Advantage through Cognitive Science and Biotechnology,” *PRISM*, 8, no. 3 (January 9, 2020), <https://ndupress.ndu.edu/Media/News/News-Article-View/Article/2053585/minds-at-war-chinas-pursuit-of-military-advantage-through-cognitive-science-and/>.

Johann Schmid, «Preface,» in *Hybrid Warfare Future and Technologies* (ZfAS ed.), ed. Ralph Thiele (Wiesbaden, DE: Springer, 2021), ix-xii.

Johann Schmid and Ralph Thiele, «Hybrid Warfare—Orchestrating the Technology Revolution,» in *NATO at 70: Outline of the Alliance Today and Tomorrow*, ed. Róbert Ondrejcsák and Tyler H. Lippert (Bratislava, SK: Strategic Policy Institute, 2019), 211-225, [https://www.stratpol.sk/wp-content/uploads/2019/12/panorama\\_2019\\_ebook.pdf](https://www.stratpol.sk/wp-content/uploads/2019/12/panorama_2019_ebook.pdf).

Frank Christian Sprengel, “Drones in Hybrid Warfare: Lessons from Current Battlefields,» *Hybrid CoE Working Paper 10*, The European Centre of Excellence for Countering Hybrid Threats, June 2021, <https://www.hybridcoe.fi/wp-content/uploads/2021/06/20210611-Hybrid-CoE-Working-Paper-10-Drones-in-hybrid-warfare-WEB.pdf>.

Ralph Thiele, ed., *Hybrid Warfare Future and Technologies* (ZfAS ed.) (Wiesbaden, DE: Springer, 2021).

Ralph Thiele, «Artificial Intelligence – A Key Enabler of Hybrid Warfare,» *Hybrid CoE Working Paper 6*, The European Centre of Excellence for Countering Hybrid Threats, March 2020, [https://www.hybridcoe.fi/wp-content/uploads/2020/07/WP-6\\_2020\\_rgb-1.pdf](https://www.hybridcoe.fi/wp-content/uploads/2020/07/WP-6_2020_rgb-1.pdf).

Ralph Thiele, “Quantum Sciences – A Disruptive Innovation in Hybrid Warfare,» *Hybrid CoE Working Paper 7*, The European Centre of Excellence for Countering Hybrid Threats, March 2020, [https://www.hybridcoe.fi/wp-content/uploads/2020/07/Working-Paper-7\\_2020.pdf](https://www.hybridcoe.fi/wp-content/uploads/2020/07/Working-Paper-7_2020.pdf).

## T2-B3: Creating and Exploiting Political, Social, and Cultural Divisions

### Description

Hybrid actions, such as Russian “active measures,” are widely used to generate or exploit political, cultural, and social divisions in the society of a targeted nation. To accomplish this task, any issue can be deliberately used and exaggerated by an adversary as a basis for a hybrid campaign. In countries targeted by a malign actor, different themes are used to cause a rift in a society. Such themes may include:

- Manipulation of common history to create the perception of legitimacy as an excuse or justification for an invasion. For example, portraying annexation or occupation of part or whole of a country’s territory as saving it from devastation by “aggressive states” or protecting an ethnic group from discrimination.
- Confrontation of outdated traditional, religious, or ideological values against other ideological values such as liberal democratic principles.
- Weaponization of migration (i.e., the “threat” of mass migration) or aggressive attitude toward migrants, including those of second and third generations.

### Background

State and nonstate actors with malign intentions can achieve strategic objectives by creating political, social, and cultural polarization to manipulate societies, create confusion, or destabilize states or international alliances and institutions. Political division is used to undermine internal cohesion and target political systems, with technology-enabled tools creating new opportunities and methods (e.g., cyber trolls and deepfakes) for delivering effects. Social division is created to undermine trust or highlight inequities in areas such as income, access to basic services, access to social protection, and social capital. Cultural elements such as ideas, customs, and behaviors are used to target, influence, recruit, divide, and ultimately manipulate communities and set them against each other, national governments, and international institutions.

Threat actors can steer public opinions and influence sizeable portions of a population by actively using malinformation and propaganda. Catalyst events can trigger violent confrontations and cause turbulence in the society.



## Learning Outcomes

Students will be able to:

- 1) Identify vulnerabilities in a targeted society that could be used by a malign actor to orchestrate hybrid activities.
- 2) Understand resilience as a countermeasure.
- 3) Understand how the preconditions for hybrid actions can be created/manipulated by using different potential historical, cultural, and social threat vectors.
- 4) Analyze political, social, and cultural divisions and vulnerabilities within one's country.

## Issues for Potential Modules and Approaches to Consider

Hybrid threats aim to undermine trust and societal cohesion; thus, methods for rebuilding trust and cohesion should be discussed and analyzed.

Some nations have difficulty agreeing on the core elements of national identity, especially during transitional periods from totalitarian regimes to liberal democratic governance or when facing a national-level crisis. The question of identity (i.e., who are we?) should be analyzed.

Political, cultural, and social divisions can be created by blurring and manipulating historical facts.

## Learning Method/Assessment

Learning methods may include lectures, guest speakers, video case studies, role playing, blogging, case studies, practical exercises, strategic games, workshops, group discussions, readings, research, article reviews, small-group exercises, and reflective journaling.

## References

Oliver Backes and Andrew Swab, *Cognitive Warfare: The Russian Threat to Election Integrity in the Baltic States*, Harvard University, Kennedy School, Belfer Center for Science and International Affairs, November 2019, <https://www.belfercenter.org/sites/default/files/2019-11/CognitiveWarfare.pdf>

Arsalan Bilal, «Hybrid Warfare–New Threats, Complexity, and ‘Trust’ as the Antidote,» *NATO Review*, November 30, 2021, <https://www.nato.int/docu/review/articles/2021/11/30/hybrid-warfare-new-threats-complexity-and-trust-as-the-antidote/index.html>.

Cedric De Coning, “Strengthening the Resilience and Adaptive Capacity of Societies at Risk of Hybrid Threats,” *Hybrid CoE Working Paper 9*, The European Centre of Excellence for Countering Hybrid Threats, June 2021, [https://www.hybridcoe.fi/wp-content/uploads/2021/05/20210601\\_Hybrid\\_CoE\\_Working\\_Paper\\_9\\_Strengthening\\_the\\_resilience\\_and\\_adaptive\\_capacity\\_of\\_societies\\_WEB.pdf/](https://www.hybridcoe.fi/wp-content/uploads/2021/05/20210601_Hybrid_CoE_Working_Paper_9_Strengthening_the_resilience_and_adaptive_capacity_of_societies_WEB.pdf/).

Leonie Haiden and Jente Althuis, eds., *Fake News: A Roadmap*, NATO Strategic Communications Centre of Excellence and King’s College London, February 28, 2018, <https://stratcomcoe.org/publications/fake-news-a-roadmap/137>. (See case studies of Russia and Daesh).

Sandra Kalniete and Tomass Pildegovičs, “Strengthening the EU’s Resilience to Hybrid Threats,» *European View*, 20, no.1 (March 25, 2021): 23-33, <https://journals.sagepub.com/doi/full/10.1177/17816858211004648>.

Katharina Krombholz, Heidelinde Hobel, Mark Huber, and Edgar Weippl, “Advanced Social Engineering Attacks,” *Journal of Information Security and Applications*, 22 (June 2015): 113-22, <https://www.sciencedirect.com/science/article/abs/pii/S2214212614001343>.

Anna Reynolds, ed., *Social Media as a Tool of Hybrid Warfare*, NATO Strategic Communications Centre of Excellence, May 2016. [https://stratcomcoe.org/cuploads/pfiles/public\\_report\\_social\\_media\\_hybrid\\_warfare\\_22-07-2016-1.pdf](https://stratcomcoe.org/cuploads/pfiles/public_report_social_media_hybrid_warfare_22-07-2016-1.pdf).

Frederik Rosén, *NATO and Cultural Property: A Hybrid Threat Perspective*, CHAC Report, Nordic Center for Cultural Heritage and Armed Conflict, March 2022, <https://www.heritageconflict.org/blog/2022/3/2/nato-and-cpp-a-hybrid-threat-perspective>.

Kim Wijnja, “Countering Hybrid Threats: Does Strategic Culture Matter?” *Defence Studies*, 22, no.1 (June 26, 2021): 16-34, <https://www.tandfonline.com/doi/full/10.1080/14702436.2021.1945452>.

Witold Waszczykowski, *The Battle for the Hearts and Minds: Countering Propaganda Attacks Against the Euro-Atlantic Community*, NATO Parliamentary Assembly, Committee on the Civil Dimension of Security, 164 CDS DG 15 E bis, October 2015, <https://www.nato-pa.int/download-file?filename=sites/default/files/documents/2015%20-%2016%20CDS DG%2015%20E%20FIN%20BIS%20-%20RUSSIAN%20PROPAGANDA%20-%20WASZCZYKOWSKI%20REPORT.doc>.

Putting People First: Practice, Challenges and Innovation in Characterizing and Mapping Social Groups, Introduction to Social Vulnerability, United Nations Development Programme, <https://understandrisk.org/wp-content/uploads/Intro-to-social-vulnerability.pdf>.

## **T2-B4: Diplomatic Tools**

### **Description**

This block helps to develop a deeper understanding of diplomacy as a tool in hybrid warfare. The classical approach to diplomacy is the art of obtaining agreement between states and actors using negotiation to resolve conflict and promote peaceful relations. The hybrid warfare vector considered here is the orchestration of diplomacy, which includes creating, targeting, and controlling a narrative.

### **Background**

Diplomacy is a tool of statecraft. The 1648 Peace of Westphalia, ending the 30 Years War, created the framework for modern international relations largely based on a balance of power and the recognition of the “state” as the formal representative of the people within it (as had not been the case during the European wars of religion). This principal was further enshrined in the United Nations (UN) Charter. The structure of the UN recognized a global balance of power through the UN Security Council. This state-to-state balance of power system remains the norm but is not without its challenges, including an increasing number of large nonstate actors, particularly transnational international terrorist, criminal, and even corporate actors.

Attempts have been made to combine elements of “traditional” diplomacy to address new challenges. For example, the Council of Europe’s Budapest Convention on Cybercrime seeks to harmonize national laws to address this new challenge. Achieving worldwide agreement has not been easy, with many countries not ratifying the Convention. Similarly, there are major challenges in determining international rules for hybrid threats. For example, some states at the UN feel that changes to the rules on Information and communications technology and information security infringe into domestic affairs.

States use diplomatic tools to support their hybrid threat activities. For example, they can prevent international investigations; vet activities across the UN, its agencies, organizations, and other international bodies; or exercise coercive public diplomacy campaigns.

## Learning Outcomes

- 1) Students will be able to:
- 2) Understand how diplomacy can be used in a hybrid format to affect international relations.
- 3) Identify examples of where diplomacy has been used with hybrid methods to influence political Goals.
- 4) Understand how diplomacy can be used in an orchestrated hybrid warfare campaign.

## Issues for Potential Modules and Approaches to Consider

An analysis of the advantages and disadvantages should be considered prior to implementing a diplomatic response to assess if the action will be detrimental or beneficial (including risks and the cost of failure) and its proportionality (i.e., instruments and effects) in relation to the hybrid threat.

Hybrid warfare and hybrid threats fit into traditional and developing notions of diplomacy (e.g., Russia reframing its role as an interested party rather than a party to the conflict in Crimea, or the Turkey-EU migration crisis to extort funding).

States can use coercive public diplomacy campaigns (e.g., Wolf-Warrior Diplomacy, Humanitarian Center as a substitute for a base in Serbia, threatening energy shutoffs, or using media as a tool of foreign policy).

States can use negative (e.g., criticism or warning), positive (e.g., a diplomatic visit or alliance with a partner state), or neutral (e.g., ignoring or suspending contact) diplomatic responses to hybrid threat vectors.

## Learning Method/Assessment

Learning methods may include lectures, guest speakers, video case studies, role playing, blogging, case studies, practical exercises, strategic games, workshops, group discussions, readings, research, article reviews, small-group exercises, and reflective journaling.

## References

The Budapest Convention (ETS No. 185) and Its Protocols, Council of Europe, accessed September 18, 2022, <https://www.coe.int/en/web/cybercrime/the-budapest-convention>.

Group of Governmental Experts, United Nations Office of Disarmament Affairs, accessed September 18, 2022, <https://www.un.org/disarmament/group-of-governmental-experts/>.

Alex Comninos, «Twitter Revolutions and Cyber Crackdowns,» Association for Progressive Communications, June 2011, [https://www.apc.org/sites/default/files/AlexComninos\\_MobileInternet.pdf](https://www.apc.org/sites/default/files/AlexComninos_MobileInternet.pdf).

Ahmad Shehabat, «The Social Media Cyber-War: The Unfolding Events in the Syrian Revolution 2011,» Global Media Journal: Australian Edition, 6, no. 2 (2012), [https://www.academia.edu/40476062/The\\_social\\_media\\_cyber\\_war\\_the\\_unfolding\\_events\\_in\\_the\\_syrian\\_revolution\\_2011](https://www.academia.edu/40476062/The_social_media_cyber_war_the_unfolding_events_in_the_syrian_revolution_2011).

Tim Sweijjs, Samuel Zilincik, Frank Bekkers, and Rick Meesen, A Framework for Cross-Domain Strategies Against Hybrid Threats, The Hague Centre for Strategic Studies, 2021, <https://euhybnet.eu/wp-content/uploads/2021/06/Framework-for-Cross-Domain-Strategies-against-Hybrid-Threats.pdf>.



## T2-B5: Economic and Financial Manipulation

### Description

This module addresses how state and nonstate actors can undermine a state's national economy through both legal and illegal actions. It addresses manipulation of both economic (i.e., local or global markets, human behavior, and goods and services) and financial systems (i.e., banks, loans, investments, and savings), which can destabilize, suppress, or co-opt these systems. It also explores how the interconnectedness of the global economy can create second-order effects in other states.

### Background

As the world economy becomes more interconnected through globalization, more opportunities emerge for economic and financial systems to be manipulated. Economic warfare can take many forms, targeting trust in the system, value and availability of currencies, economic foundations, and productivity of an economy. Financial systems can be used as weapons to advance geopolitical objectives (e.g., affecting capital flows or infiltrating financial centers) and/or create chaos (e.g., triggering a financial crisis on stock exchanges).

Potential areas for economic and financial system discussion include, but are not limited to:

- Governmental and international agencies regulating banks;
- Pressure on critical infrastructure;
- Supply chain infiltration or manipulation (e.g., counterfeit goods or malware insertion);
- Foreign trade zones, offshore companies, foreign direct investments, and tax havens;
- Money laundering;
- Malware against economic and financial systems (e.g., ransomware or cyber theft);
- Misuse of cryptocurrencies and non-fungible tokens;
- Remittances (e.g., migrant income flowing back to country of origin), and
- Non-tangible assets (e.g., intellectual property, patents, or research).

Some states use trade, aid, investments, and threats of sanctions to influence state behavior in contested regions. Economic responses by states to economic and financial coercion include retaliatory sanctions, blockades, and embargoes.

Multinational technology and social media platforms (e.g., Amazon, Google, Meta, and Apple), which now have a financial turnover greater than the gross domestic product (GDP) of many countries of the world, should also be considered. The social media platforms have tremendous power and influence in politics and commerce. At the same time, technology and social media platforms have enabled individuals and groups to shape national and even international affairs online.

### Learning Outcomes

Students will be able to:

- 1) Understand that economic and financial means can be used to destabilize national economies through the manipulation of different systems.
- 2) Explore ways that states have used economic and financial actions to advance geopolitical objectives.

### Issues for Potential Modules and Approaches to Consider

Economic and financial systems can be utilized as means and methods to attack by manipulating, disrupting, and/or obstructing access.

Economic and financial systems are interconnected with a nation's critical infrastructure and can have widespread impact on a nation.

The use of diplomatic responses such as sanctions, blockades, and embargoes may be considered.

Not all financial systems are trackable (e.g., remittances), thereby rendering diplomatic tools ineffective and/or increasing the opportunities for illegal flows of funding.

### Learning Method/Assessment

Learning methods may include lectures, guest speakers, video case studies, role playing, blogging, case studies, practical exercises, strategic games, workshops, group discussions, readings, research, article reviews, small-group exercises, and reflective journaling.

## References

Aleksi Aho, Catarina Midoes, and Arnis Snore, Hybrid Threats in the Financial System, Hybrid CoE Working Paper 8, The European Centre of Excellence for Countering Hybrid Threats, June 2020, [https://www.hybridcoe.fi/wp-content/uploads/2020/07/20200630\\_Working-Paper-8\\_Web-1.pdf](https://www.hybridcoe.fi/wp-content/uploads/2020/07/20200630_Working-Paper-8_Web-1.pdf).

Sara Dudley, Steve Ferenzi, Travis Clemens, "Financial Access Denial. An Irregular Approach to Integrated Deterrence," *Military Review*, (March-April, 2023), pp. 43-55.

Jan Famfollet, Richard Kraemer, František Marčík, and Jakub Janda, How to Protect the Czech Economy from Foreign Predators and Malign Influence, European Values Center for Security Policy, 2021, <https://europeanvalues.cz/wp-content/uploads/2021/11/Protecting-Czech-Economy-from-Foreign-Predators-and-Malign-Influence-2021.pdf>.

Elmar Hellendoorn, Financial Geopolitics and Hybrid Conflict: Strategic Competition in a Financialized World, Hybrid CoE Working Paper 16, European Centre of Excellence for Countering Hybrid Threats, April 2022, <https://www.hybridcoe.fi/wp-content/uploads/2022/04/Hybrid-CoE-Working-Paper-16-Financial-geopolitics-WEB.pdf>.

Lucia Retter, Erik J. Frinking, Stijn Hoorens, Alice Lynch, Fook Nederveen, and William D. Phillips, Relationships Between the Economy and National Security: Analysis and Considerations for Economic Security Policy in the Netherlands (Cambridge, UK: RAND Europe, 2020), [https://www.rand.org/pubs/research\\_reports/RR4287.html](https://www.rand.org/pubs/research_reports/RR4287.html).

Christopher Sims, "The Evolution of Economic Compellence," *Military Review* (July-August 2021), pp. 44-51.

## T2-B6: Military Vectors

### Description

Hybrid warfare actors tend to operate in the shadows of the interfaces between war and peace, friend and foe, internal and external security, and civil and military entities, as well as state and nonstate actors. They tend to design their military vectors accordingly to be able to operate at such interfaces. These operations may include the use of regular, irregular, and proxy forces; overt and/or covert military operations; or symmetric and asymmetric warfighting potentially on all levels of escalation. Show of force and projection of force, as well as the threat of the use of military force, could be as important as the active employment of military means and methods. Combining different modes of warfare and recognizing lethal and nonlethal (kinetic and non-kinetic) elements are vital parts of hybrid warfare.

### Background

Conventional military forces may not be structured to recognize or respond to hybrid threats below the threshold of the use of force; therefore, they may not be mandated or optimized to address the full range of challenges with hybrid threats. However, conventional military forces can play an important role in addressing hybrid threats and hybrid warfare. Specialized forces may play a critical role in responding to nonlethal and non-kinetic threat vectors. The military sphere also has seen the increased presence of proxy paramilitary organizations, private military/security companies (some with close ties to government authorities), various extremist armed groups, and volunteer militias or nationalist separatist armed formations.

The capabilities of nonmilitary intelligence or security services may be essential for a comprehensive response to hybrid efforts. These capabilities require close coordination, in mutual support, and may be synchronized with military elements. Thus, intelligence and security services actions can also be considered as part of the military hybrid-threat vector.

### Learning Outcomes

Students will be able to:

- 1) Understand the military component of hybrid warfare.
- 2) Understand military proxy forces: their types, composition, order of battle and tactics, techniques, and procedures.

- 3) Identify the difference between military proxy forces and non-military proxy elements in hybrid warfare.
- 4) Understand that the military threat vector includes intelligence or security services support, which is waged in close coordination, in mutual support, and synchronized with military elements.

### **Issues for Potential Modules and Approaches to Consider**

States can use their military capabilities (conventional and nuclear) for shielding their hybrid activities from interference by third countries or international organizations.

Irregular or proxy military forces are characterized as uncertain, complex, and ambiguous (e.g., nondoctrinal composition, disposition, and capabilities).

Generally, military components of hybrid warfare are less active and observable in the first stages of hybrid activities, but they may play decisive roles in the final stages during rapid vertical and horizontal escalation of the situation.

### **Learning Method/Assessment**

Learning methods may include lectures, guest speakers, video case studies, role playing, blogging, case studies, practical exercises, strategic games, workshops, group discussions, readings, research, article reviews, small-group exercises, and reflective journaling.

### **References**

Otto C. Fiala, ed., *Resistance Operating Concept* (Stockholm, SE: Special Operations Command Europe, 2019), <https://www.diva-portal.org/smash/get/diva2:1392106/FULLTEXT01.pdf>.

Brian P. Fleming, *Hybrid Threat Concept: Contemporary War, Military Planning and the Advent of Unrestricted Operational Art*, School of Advanced Military Studies Monograph, ADA545789, Army Command and General Staff College, May 19, 2011, <https://apps.dtic.mil/sti/citations/ADA545789>.

Sean Monaghan, "Countering Hybrid Warfare: So What for the Future Joint Force?" *Prism* 8, no. 2 (October 2019): 82-98, [https://ndupress.ndu.edu/Portals/68/Documents/prism/prism\\_8-2/PRISM\\_8-2\\_Monaghan.pdf](https://ndupress.ndu.edu/Portals/68/Documents/prism/prism_8-2/PRISM_8-2_Monaghan.pdf).

Johann Schmid, "Hybrid Warfare in Vietnam – How to Win a War Despite Military Defeat," *ISPAIM-Monitor Strategic*, B.Nr. 17 (February 12, 2020): 54-67, [https://www.hybridcoe.fi/wp-content/uploads/2021/03/210302\\_HW-in-Vietnam\\_table-of-content.pdf](https://www.hybridcoe.fi/wp-content/uploads/2021/03/210302_HW-in-Vietnam_table-of-content.pdf).

Johann Schmid, "Hybrid Warfare on the Ukrainian Battlefield: Developing Theory Based on Empirical Evidence." *Journal on Baltic Security*, 5, no. 1 (2019): 5-15, [https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/resources/docs/BDC\\_1\\_23829230%20-%20Journal%20on%20Baltic%20Security%20Hybrid%20warfare%20on%20the%20Ukrainian%20battlefield\\_%20developing%20theory%20based%20on%20empirical%20evidence.pdf](https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/resources/docs/BDC_1_23829230%20-%20Journal%20on%20Baltic%20Security%20Hybrid%20warfare%20on%20the%20Ukrainian%20battlefield_%20developing%20theory%20based%20on%20empirical%20evidence.pdf).

Frank Christian Sprengel, "Drones in Hybrid Warfare: Lessons from Current Battlefields," Hybrid CoE Working Paper 10, The European Centre of Excellence for Countering Hybrid Threats, June 2021, [https://www.hybridcoe.fi/wp-content/uploads/2021/06/20210611\\_Hybrid\\_CoE\\_Working\\_Paper\\_10\\_Drones\\_in\\_hybrid\\_warfare\\_WEB.pdf](https://www.hybridcoe.fi/wp-content/uploads/2021/06/20210611_Hybrid_CoE_Working_Paper_10_Drones_in_hybrid_warfare_WEB.pdf).



## T2-B7: Proxy Forces

### Description

A wide range of organized groups, including states, can be used as proxy forces under a common umbrella of hybrid activities against a targeted country. This section examines the different types of proxy forces and some of the ways in which they may be employed.

### Background

Proxy forces, in addition to military or paramilitary elements, can conduct “active measures” (e.g., covert operations to influence political attitudes and public opinion) within a country that has been targeted with hybrid warfare. These proxy forces use different spheres of influence to set up the conditions for hybrid activities. At the same time, proxy forces can be used after certain hybrid actions (e.g., to consolidate gains). Proxy forces can be used to transform a country into a client and puppet state.

Nonmilitary proxy forces could include political parties and various civil society organizations (non-governmental organizations-NGOs), criminal armed groups, and illicit networks that can support and promote the agendas of hybrid warfare. Financial and political support, as well as media coverage, can be leveraged to bolster such groups. Proxy actors may be NGOs affiliated with the hybrid attacker. Wittingly or not, their activities may include the following facets: research in support of relations with the protracting [or expanding/encroaching?] country, sounding the ideas or options of political vectors previously unacceptable in the society, and establishing ideological preconditions for the creation of organized interest groups. Prominent figures, religious institutions, and theological schools can be used as a strong source for influencing wide segments of society and legitimizing actions, especially within countries or enclaves with strong religious beliefs.

Hybrid threats and warfare often include a combination of different kinds of actors: state and nonstate actors. These actors can use each other as proxies, enabling operations by creating ambiguity and plausible deniability. (The term “Fifth Column” is sometimes used to collectively describe proxy forces in a targeted country.)

### Learning Outcomes

Students will be able to:

- 1) Examine the role of nonmilitary proxy forces during different stages of hybrid activities.
- 2) Understand that behind a facade of political, religious, non-governmental, or other organizations there may be proxy elements engaging in hybrid warfare.
- 3) Identify covert connections between certain political, non-governmental, or religious organizations as part of hybrid activities.

### Issues for Potential Modules and Approaches to Consider

Countering proxy forces will involve close coordination with nontraditional partners (local government, justice ministries, civil society, media, and the private sector, etc.).

Military use of proxy forces in different contexts (e.g., “little green men” used in Ukraine, Axis of Resistance militia and paramilitary forces used in the Levant, and civilian fishing boats used in the South China Sea to provoke targeted states).

States and nonstate actors can exploit the services of a private company, which can operate as a proxy for a state. For example, for-profit intelligence services (e.g., spyware from Pegasus, the technology firm that offered services enabling state and nonstate actors to spy on journalists and activists) offer important lessons for policymakers, researchers, and activists regarding privacy and human rights online. Private contractors (e.g., Wagner Group or the Internet Research Agency) can also operate in close coordination with a state’s military to conduct its operations.

### Learning Method/Assessment

Learning methods may include lectures, guest speakers, video case studies, role playing, blogging, case studies, practical exercises, strategic games, workshops, group discussions, readings, research, article reviews, small-group exercises, and reflective journaling.

## References

William Akoto, «Hackers for Hire: Proxy Warfare in the Cyber Realm,» Modern War Institute, January 31, 2022, <https://mwi.usma.edu/hackers-for-hire-proxy-warfare-in-the-cyber-realm/> and [https://www2.fireeye.com/rs/848-DID-242/images/rpt\\_APT37.pdf](https://www2.fireeye.com/rs/848-DID-242/images/rpt_APT37.pdf).

Matt Tait, Runa Sandvik, and Tarah Wheeler, «Lessons for Policymakers from the NSO Group Saga,» TechStream, Brookings Institution, January 19, 2022, <https://www.brookings.edu/techstream/lessons-for-policymakers-from-the-nso-group-saga/>.

Brandon Valeriano and Jose Macias, «Paper Tigers: Proxy Actors Are the True Cyber Threats,» CATO Institute, April 12, 2022, <https://www.cato.org/commentary/paper-tigers-proxy-actors-are-true-cyber-threats>.

Mikael Wigell, Harri Mikkola, and Tapio Juntunen, Best Practices in the Whole-of-Society Approach in Countering Hybrid Threats, EP/EXPO/INGE/FWC/2019-1/LOT6/R/06 Report, European Union, May 6, 2021, [https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653632/EXPO\\_STU\(2021\)653632\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653632/EXPO_STU(2021)653632_EN.pdf)

## T2-B8: Organized Crime

### Description

Organized crime groups increasingly present hybrid threats. This module introduces the breadth of criminal activities, the networks that support them, the coercive tactics used to advance their objectives, and the effects the criminal groups have on society.

### Background

Gangs, vigilantes, cartels, and criminal organizations use coercive tactics to create social and political destabilization within states and between states. These coercive tactics are manifested in many different forms (e.g., narcotrafficking, maritime piracy, human trafficking, irregular/illegal migration, and cybercrime) to pursue an organization's objectives. The primary objective of groups involved in organized crime is monetary profit and economic power, often through more than one criminal activity. Behind every organized crime group is a network of facilitators helping the group enable its activities or evade law enforcement and including money launderers, customers, financial brokers, and attorneys. Technological enablers, such as encryption, cryptocurrency, and the dark web, enable these groups to operate more expansively and to evade detection. These enablers also lower the barriers for the establishment of criminal organizations. Furthermore, organized crime groups can be leveraged by state-sponsored or nonstate groups to advance their strategic objectives.

Organized crime groups thrive in weak, fragile, and failed states because they can operate freely due to weak governance. They intentionally shape the environment using strategies, such as corruption and violence, to pressure the state and intimidate the population. Additionally, their use of violence can destabilize regions, causing mass migration to escape the violence. Organized crime groups also use legal and illegal means to undermine the rule of law and stability to advance their objectives, which can be done in conjunction with a state or to undermine a targeted state. Finally, in some situations, they can take the role of a quasi-state when an official state is unable to provide the political goods and services to its people (e.g., designated terrorist groups that serve as de facto governments).

## Learning Outcomes

Students will be able to:

- 1) Consider the coercive tactics that can be used by criminal organizations to create social and political unrest.
- 2) Understand that, while law enforcement and security services play a role in responding to criminal organizations, a whole-of-society approach is preferred.

## Issues for Potential Modules and Approaches to Consider

Analyze criminal activities in a targeted state (e.g., narco-trafficking, maritime piracy, and human trafficking).

Organized crime groups can be used to undermine institutions and governance in a targeted state (e.g., criminal gangs exercising control over the civilian population in the Donbas in 2014).

Organized crime groups conduct a wide variety of activities that have political effects in targeted nations: ransomware against critical infrastructures (e.g., SolarWinds), bank heist (e.g., Central Bank of Bangladesh 2017), foreign election tampering (e.g., U.S. presidential election in 2016), or hacktivism against a state (e.g., Anonymous in 2021 Ukraine conflict).

## Learning Method/Assessment

Learning methods may include lectures, guest speakers, video case studies, role playing, blogging, case studies, practical exercises, strategic games, workshops, group discussions, readings, research, article reviews, small-group exercises, and reflective journaling.

## References

Sascha-Dominik Bachmann, "Is the Belarus Migrant Crisis a 'New Type of War'? A Conflict Expert Explains," The Conversation, November 16, 2021, <https://theconversation.com/is-the-belarus-migrantcrisis-a-new-type-of-war-a-conflict-expert-explains-171739>.

Paulina Rios Maya, «The Narco Hybrid-Threat,» Small Wars Journal, March 18, 2021, <https://smallwarsjournal.com/jrnl/art/narco-hybrid-threat>.

David H. Ucko and Thomas A. Marks, Organised Crime as Irregular Warfare: Strategic Lessons for Assessment and Response, SOC ACE Research Paper

No. 4, University of Birmingham, 2022, <https://www.birmingham.ac.uk/documents/college-social-sciences/government-society/publications/organised-crime-irregular-warfare-report.pdf>.

Hybrid Threats: A Strategic Communications Perspective, NATO Strategic Communications Centre of Excellence, 2019, [https://stratcomcoe.org/cuploads/pfiles/2nd\\_book\\_short\\_digi\\_pdf.pdf](https://stratcomcoe.org/cuploads/pfiles/2nd_book_short_digi_pdf.pdf).

MCDC Countering Hybrid Warfare Project, "A Deadlier Peril': The Role of Corruption in Hybrid Warfare," MCDC Countering Hybrid Warfare Project Information Note, Multinational Capability Development Campaign, March 2019, [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/795222/20190318-MCDC\\_CHW\\_Info\\_note\\_7.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/795222/20190318-MCDC_CHW_Info_note_7.pdf).

"Theoretical Frameworks on the Linkages between Organized Crime and Terrorism,» E4J University Module Series: Organized Crime / Counter-Terrorism, Module 16, United Nations Office on Drugs and Crime, March 2019, <https://www.unodc.org/e4j/en/organized-crime/module-16/key-issues/theoretical-frameworks-on-the-linkages-between-organized-crime-and-terrorism.html>.



## T2-B9: Lawfare

### Description

This module explores lawfare, which is the use of law as a weapon against an adversary. Specifically, it is the use or misuse of international norms and laws as a non-kinetic weapon to achieve political Goals. Malign state and nonstate actors are exploiting legal mechanisms as an unconventional means to achieving their strategic objectives. This module also delves into the multifaceted challenges that lawfare poses for law-abiding states.

### Background

Military engagements are commonly guided by national and internationally agreed-upon rules of engagement, most of which address the use of deadly force. Malign actors use hybrid warfare to exploit legalities to achieve their strategic objectives using domestic and international law, along with other commercial and regulatory rules or standards. The following are modern examples of methods used to achieve strategic objectives or usurp international rules-based order:

Human migration can be used to create a refugee crisis as a form of weaponized migration. In this instance, malign actors exploit customary international law for human rights (i.e., the right of asylum and the principle of racial nondiscrimination).

States can misuse International Criminal Police Organization (INTERPOL) red notices, which are international arrest alerts to law enforcement, to target political opponents and human rights defenders (e.g., journalists). States issue red notices to have a third-party country detain and extradite individuals back to their home country. When the red notice system is abused (e.g., to locate and/or harass political opponents), it can result in violations of international human rights standards.

States or nonstate actors can infringe into other states' economic exclusion zone (EEZ) to engage in illegal, unreported, and unregulated (IUU) fishing. These malign actors intentionally turn off their automated identification systems while fishing and ignore international norms and local regulations. In addition, some malign actors also exploit the law-abidingness of other states by intentionally using a maritime militia to occupy the seas around contested islands, provoking and ramming into commercial and military vessels.

### Learning Outcomes

Students will be able to:

- 1) Understand how legal mechanisms can be misused to pursue the strategic objectives of malign actors.
- 2) Examine how law-abiding states are challenged by malign actors who exploit international norms, rules, and laws.

### Issues for Potential Modules and Approaches to Consider

Lawfare does not necessarily involve litigation and can take many forms (e.g., the assertion of a legal theory followed by kinetic action, as seen in the South China Sea, and the misuse of established norms or conduct), thereby creating a new system of understanding.

Lawfare includes malign actors' attempts to dominate international bodies (e.g., the World Health Organization or the International Telecommunication Union) to either control the agenda for discussion or change international order.

Malign actors promote their actions as lawful and their opponents' reactions as unlawful, thereby putting a law-abiding state at a disadvantage.

Lawfare countermeasures are not necessarily limited to the recalibration of legal or regulatory frameworks enabling the abuse. Decision makers must exercise creativity to overcome lawfare challenges.

### Learning Method/Assessment

Learning methods may include lectures, guest speakers, video case studies, role playing, blogging, case studies, practical exercises, strategic games, workshops, group discussions, readings, research, article reviews, small-group exercises, and reflective journaling.

### References

- Udayvir Ahuja, «China Resorts to Lawfare: A New Maritime Policy,» Observer Research Foundation, November 16, 2021, <https://www.orfonline.org/expert-speak/china-resorts-to-lawfare-a-new-maritime-policy/>.
- Matthew Anderson, «Belarus's Lawfare Against Latvia, Lithuania and Poland,» Lawfare, October 25, 2021, <https://www.lawfareblog.com/belarus-lawfare-against-latvia-lithuania-and-poland>.

Andres B. Munoz Mosquera and Sascha Dov Bachmann, «Lawfare in Hybrid Wars: The 21st Century Warfare.» *Journal of International Humanitarian Legal Studies*, 7, no. 1 (March 14, 2016): 63-87, [https://brill.com/view/journals/ihls/7/1/article-p63\\_4.xml](https://brill.com/view/journals/ihls/7/1/article-p63_4.xml).

Aurel Sari, «Hybrid Threats and the Law: Building Legal Resilience,» Hybrid CoE Research Report 3, The European Centre of Excellence for Countering Hybrid Threats, November 4, 2021, [https://www.hybridcoe.fi/wp-content/uploads/2021/10/20211104\\_Hybrid\\_CoE\\_Research\\_Report\\_3\\_Hybrid\\_threats\\_and\\_the\\_law\\_WEB.pdf](https://www.hybridcoe.fi/wp-content/uploads/2021/10/20211104_Hybrid_CoE_Research_Report_3_Hybrid_threats_and_the_law_WEB.pdf).

Tim Sweijts, Samuel Zilincik, Frank Bekkers, and Rick Meessen, A Framework for Cross-Domain Strategies Against Hybrid Threats, The Hague Centre for Strategic Studies, 2021, <https://euhybnet.eu/wp-content/uploads/2021/06/Framework-for-Cross-Domain-Strategies-against-Hybrid-Threats.pdf>.

## T2-B10: Putting It All Together

### Description

In Theme 2, a variety of vectors (means and methods) to execute a hybrid warfare approach were covered. Hybrid actors use a blend of these vectors to gain an asymmetric and/or symmetric advantage. By employing a multitude of attack vectors, as well as orchestrated multi-vector attacks, they can use the military and non-military domains to achieve strategic objectives. This module explores approaches that states use to address the complex security challenge posed by hybrid warfare.

### Background

State and nonstate actors are constantly adapting so that they may unleash new forms of hybrid threats to challenge international norms and laws to achieve their Goals. They aim to progressively achieve their objectives without necessarily provoking a decisive response. They target states' vulnerabilities (government, private sector, and civilians) using a broad array of violent and nonviolent approaches. Hybrid threats cross into civil society to apply political pressure on the targeted state. As a result, hybrid threats create complex security challenges that cannot be adequately addressed with just military or civilian responses. A whole-of-state and whole-of-society approach is necessary to address societal vulnerabilities and build resilience against hybrid threats/attacks.

States face the formidable task of detecting, deterring, and responding to hybrid threats, without provoking or escalating threat actor activities. As a result, they need to have increased domestic and international cooperation, as well as robust information-sharing capabilities with partners and allies. Given the wide-ranging, evolving nature of hybrid threats, states should be developing resilience to withstand and minimize the disruptive event.

### Learning Outcomes

Students will be able to:

- 1) Understand that a combination of hybrid threats/vectors can be used to increase political pressure on a targeted state.
- 2) Examine how hybrid threats can have spillover effects into neighboring countries, alliances, and partnerships.

- 3) Summarize the threat vectors and their impact on multiple domains.
- 4) Discuss the future evolution of hybrid threats and warfare.

### **Issues for Potential Modules and Approaches to Consider**

Hybrid threats do not manifest immediately. Often-times, there is a gradual escalation of activities (e.g., South China Sea territorial disputes or Ukraine from 2014 to present) for which the multi-vector impacts are latent.

Building governmental and societal resilience to hybrid threats involves a whole-of-government/society approach.

While information sharing is essential to better detect, deter, and respond to hybrid threats at the international, regional, and national levels, it can be hindered by lack of trust and legal, technical, and procedural differences (e.g., what to share, with whom to share, why to share, how to share, and methods of sharing).

### **Learning Method/Assessment**

Learning methods may include lectures, guest speakers, video case studies, role playing, blogging, case studies, practical exercises, strategic games, workshops, group discussions, readings, research, article reviews, small-group exercises, and reflective journaling.

### **References**

Janne Jokinen and Magnus Normark, Hybrid Threats from Non-state Actors: A Taxonomy, Hybrid CoE Research Report 6, The European Centre of Excellence for Countering Hybrid Threats, June 2022, <https://www.hybridcoe.fi/wp-content/uploads/2022/05/20220609-Hybrid-CoE-Research-Report-6-Non-state-actors-WEB.pdf>.

Sean Monaghan, "Countering Hybrid Warfare: So What for the Future Joint Force?" Prism 8, no. 2 (October 2019): 82-98, [https://ndupress.ndu.edu/Portals/68/Documents/prism/prism\\_8-2/PRISM\\_8-2\\_Monaghan.pdf](https://ndupress.ndu.edu/Portals/68/Documents/prism/prism_8-2/PRISM_8-2_Monaghan.pdf).

Todor Tagarev, "Understanding Hybrid Influence: Emerging Analysis Frameworks," in Digital Transformation, Cyber Security and Resilience of Modern Societies, eds. Todor Tagarev, Krassimir

Atanasov, Vyacheslav Kharchenko, and Janusz Kasprzyk (Cham, CH: Springer, 2021), 449-63.

Dick Zandee, Sico van der Meer, and Adája Stoetman, Countering Hybrid Threats: Steps for Improving EU-NATO Cooperation, Clingendael Report, Netherlands Institute of International Relations, October 2021, <https://www.clingendael.org/sites/default/files/2021-10/countering-hybrid-threats.pdf>.

European Commission, Mapping of Measures Related to Enhancing Resilience and Countering Hybrid Threats, Joint Staff Working Document, SWD(2020) 152 final, High Representative of the Union for Foreign Affairs and Security Policy, July 24, 2020, [https://www.europarl.europa.eu/RegData/docs\\_autres\\_institutions/commission\\_europeenne/swd/2020/0152/COM\\_SWD\(2020\)0152\\_EN.pdf](https://www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/swd/2020/0152/COM_SWD(2020)0152_EN.pdf).

National Commission on Terrorist Attacks upon the United States, The 9/11 Commission Report (Washington, DC: Government Printing Office, 2004), 399-428, <https://9-11commission.gov/report/>.





Hybrid Threats and Hybrid Warfare Reference Curriculum Writing Team Workshop, Garmisch-Partenkirchen, February 2022.



Hybrid Threats and Hybrid Warfare Reference Curriculum Writing Team Workshop, Garmisch-Partenkirchen, February 2022.







### Theme 3 – Actors: From Great Powers and Small States to Nonstate and Proxy Actors

#### Goal

Various actors use the means and methods of presenting hybrid threats or executing a hybrid warfare campaign that were explored in Theme Two. This theme introduces the dominant actors in the hybrid threat/hybrid warfare space, then turns to intergovernmental, small state, nonstate, and proxy actors.

#### Description

In this section we explore the use of hybrid threats, warfare, and influence by state and nonstate actors in the current era of heightened great power competition. We explore unique characteristics of that competition and its challenges to and effects on international cooperation and multilateralism. Great power competition may dominate international relations, but smaller states and nonstate actors, even those relatively well-armed or with advanced economies, are subject to persistent rivalry. As a result of this persistent rivalry, state and nonstate actors may employ hybrid threats and hybrid warfare. A comprehensive understanding of such threats may be used to develop the mitigation and social resilience strategies and measures addressed in Theme 4.

#### Background

Members of international organizations, such as the UN, NATO, or the EU, have clear common interests but also have conflicting national interests. Friction between competing interests greatly increases the relevance of hybrid threats and hybrid warfare.

Hybrid warfare, hybrid threats, and gray area conflict challenge the traditional understanding of the current world order and international norms. In particular, hybrid threats and warfare call into question the distinction between state and nonstate actors, the standard dichotomy between war and peace, and even the “great power” concept. (Although this curriculum does not seek to resolve the ongoing debate on great power, we recommend Paul Kennedy’s *The Rise and Fall of the Great Powers* for a solid introduction and historical discussion of the concept.)

Most nations that will employ this reference curriculum are not among the current commonly accepted great powers (the United States, the People’s Republic of

China, or Russia)—yet allies of these powers and those who live near or have geopolitical and historical relations with these powers are impacted by their actions and designs for influence and authority. Moreover, in this shifting global environment, new powers could potentially emerge.

#### Broad Objectives

In blocks 1-8, we take a closer look at the articulated hybrid threat/hybrid warfare policies of the United States, the People’s Republic of China (PRC), and Russia. We then address the role of and challenges to midsize and small states, nonstate actors such as criminal networks, and proxy actors. Understanding this broad range of actors may help build a more comprehensive view of the activity and threat spectrums subsumed under the hybrid threat, hybrid warfare, and influence labels.

#### Learning Objectives

Students will be able to:

- 1) Describe the shifting nature of the global order.
- 2) Identify the variety of entities engaged in and affected by hybrid threats/hybrid warfare (different sized states, networks, criminal organizations, non-governmental organizations, nonstate actors, and supranational organizations and companies).
- 3) Understand the interconnected ecosystem of modern conflict and the institutions that address the interacting elements.
- 4) Demonstrate an understanding of the vulnerability, fragility, and resilience of modern institutions, economies, and societies.
- 5) Demonstrate an understanding of the concept of “great power competition” in the context of hybrid threats/hybrid warfare.
- 6) Demonstrate familiarity with key insights into American, Chinese, and Russian contemporary conflict theories that focus on hybrid warfare and hybrid threats.
- 7) Evaluate nations within the geopolitical dimensions of great power competition and highlight the common and nationally unique features within that geopolitical space.



## Suggested References

- Philip C. Bobbitt, *The Shield of Achilles: War, Peace, and the Course of History* (New York: Anchor, 2003).
- Robert J. Bunker and John P. Sullivan, eds. *Illicit Tactical Progress: Mexican Cartel Tactical Notes 2013-2021* (Bloomington, IN: Xlibris, 2021).
- Manuel Castells, *The Information Age: Economy, Society and Culture*, three-volume series from Wiley: *The Rise of the Network Society*, Volume I (1996); *The Power of Identity*, Volume II (1997); *End of Millennium*, Volume III (1998).
- Manuel Castells, *Communication Power* (Oxford: Oxford University Press, 2013).
- James Cockayne, *Hidden Power: The Strategic Logic of Organized Crime* (Oxford: Oxford University Press, 2016).
- Nathan Freire, «Strategic Competition and Resistance in the 21st Century: Irregular, Catastrophic, Traditional, and Hybrid Challenges in Context», MA diss, U.S. Army War College, Strategic Studies Institute, <https://www.files.ethz.ch/isn/32058/Strategic%20Competition%20Resistance.pdf>.
- Luis Jorge Garay, Eduardo Salcedo-Albarán, and Isaac De León-Beltrán, «From State Capture Towards the Co-opted State Reconfiguration», SSRN Electronic Journal, May 2009 (Series at ResearchGate), [https://www.researchgate.net/publication/256012836\\_From\\_State\\_Capture\\_towards\\_the\\_Co-opted\\_State\\_Reconfiguration\\_An\\_Analytical\\_Synthesis](https://www.researchgate.net/publication/256012836_From_State_Capture_towards_the_Co-opted_State_Reconfiguration_An_Analytical_Synthesis).
- Mark Galeotti, «In Moscow's Shadows 83: Putin's Decision-making and Russian Organised Crime after the Invasion», podcast, November 13, 2022, <https://podcasts.apple.com/gb/podcast/in-moscows-shadows-83-putins-decision-making-and/id1510124746?i=1000586007396>.
- Mark Galeotti, «In Moscow's Shadows 61: Ukraine: When Autocracy Meets Technocracy–Putin's War, Info War, Spook War», podcast, March 12, 2022, <https://podcasts.apple.com/gb/podcast/in-moscows-shadows-61-ukraine-when-autocracy-meets/id1510124746?i=1000553796270>.
- Mark Galeotti, *The Weaponisation of Everything: A Field Guide to the New Way of War* (New Haven, CT: Yale University Press, 2022).
- Mark Galeotti, *Putin's Wars – From Chechnya to Ukraine* (Oxford: Osprey Publishing, 2022).
- Nils Gilman, Jesse Goldhammer, and Steven Weber, eds., *Deviant Globalization: Black Market Economy in the 21st Century* (New York: Continuum, 2011).
- Dr. Larry Goodson, Kautilya, U.S. Army War College, September 2014, video link: Kautilya and the Arthashastra: Lessons in Statecraft–YouTube.
- Adam Isacson, «Great-Power Competition Comes for Latin America», War on the Rocks, February 24, 2022, <https://warontherocks.com/2022/02/great-power-competition-comes-for-latin-america/>.
- Bruce Jones, «Major Power Rivalry and the Management of Global Threats», Council on Foreign Relations, November 2021, <https://www.cfr.org/report/major-power-rivalry-and-management-global-threats>.
- Matej Kandrik, «The Case Against the Concept of Great Power Competition», The Strategy Bridge, June 2021, <https://thestategybridge.org/the-bridge/2021/6/30/the-case-against-the-concept-of-great-power-competition>.
- Paul Kennedy, *The Rise and Fall of the Great Powers*, (New York: Random House, 1987).
- Stephen Kieninger, «George Shultz and the Road to the INF Treaty. Process and Personal Diplomacy», Hoover Institution, December 2020, <https://www.hoover.org/research/george-shultz-and-road-inf-treaty-process-and-personal-diplomacy>.
- Louise Shelly, *Dirty Entanglements: Corruption, Crime, and Terrorism* (Cambridge: Cambridge University Press, 2014).
- John P. Sullivan and Robert J. Bunker, eds. *The Rise of the Narcostate (Mafia States)* (Bloomington, IN: Xlibris, 2018).
- John P. Sullivan and Robert J. Bunker, eds. *Competition in Order and Progress: Criminal Insurgencies and Governance in Brazil* (Bloomington, IN: Xlibris, 2022).
- John P. Sullivan, «How Illicit Networks Influence Sovereignty», chapter 10 in *Convergence: Illicit Networks and National Security in the Age of Globalization*, eds. Michael Miklaucis and Jacqueline Brewer (Washington, DC: National Defense University Press, 2013).
- Kenneth Watkin, *Fighting at the Legal Boundaries: Controlling the Use of Force* (Oxford: Oxford University Press, 2016).

### T3-B1: The United States

#### Description

Like other nations, the United States has found itself the target of hybrid threats and has been accused of engaging in both hybrid threats and hybrid warfare. This block focuses on two broad issues. The first focus is on the challenges the United States is facing in the context of Hybrid Warfare. The second focus is on the United States as an external actor that engages in what it terms irregular and political warfare.

The United States is a large, federal democracy made up of 50 states and 5 territories. It also has the most expensive and possibly most powerful military in the world and a large, sophisticated defence industrial complex. Thus, many bureaucratic and political entities are involved in defence, homeland security, intelligence, policing, emergency management, and diplomacy.

The institutional complexity of the United States can present challenges. A broad range of state agencies is responsible for detecting, mitigating, and defending against hybrid threats and hybrid warfare. Federal agencies—such as the State Department, Federal Bureau of Investigation, Homeland Security, and the U.S. Treasury—and local state and city law enforcement agencies, as well as various rule-of-law institutions including state prosecutors and state National Guard formations, may all play a role; the budget of the New York City police force, for example, rivals the defence budget of some NATO members. However, national coordination is a challenge. It might appear logical to nationally harness the many disparate intelligence and policing bodies to employ their important and unique capabilities (domestic intelligence, community policing, investigations, public order maintenance, border security, and stability polling units, etc.), but no central agency is doing so. (Students may wish to explore why this gap exists.)

Conceptually, the United States does not have an agreed-upon lexicon for hybrid threats or hybrid warfare. Although the terms are used occasionally in official government literature, no single definition is agreed upon among U.S. Government agencies. The U.S. military tends to favor the term “gray area” warfare, but that term is not formally employed. The official military term that comes closest to hybrid warfare is “irregular warfare,” while the Central Intelligence Agency employs the term “political warfare.” The terms gray area warfare, irregular warfare, and political warfare should all be addressed in this theme.

Externally, given its strategic interests and vast international footprint, the United States has demonstrated a proactive foreign policy that is status quo-oriented. U.S. policy, however, is also informed by the concept of “American Exceptionalism” as the vital champion of the rules-based international order, as seen in various National Security Strategy statements.

#### Learning Outcomes

Students will be able to:

- 1) Demonstrate familiarity with current U.S. national security policies regarding great power conflict, hybrid warfare, and hybrid threats.
- 2) Demonstrate they have reviewed the complex national security apparatus of the United States, including the capabilities the United States can provide to a coalition operation and their limitations.
- 3) Demonstrate they have explored the concepts of irregular and political warfare as found in U.S. Government sources.

#### Issues for Potential Modules and Approaches to Consider

The SMEs using this reference curriculum will have to judge how much detail they provide their students on the internal security structures of the United States, as this issue may be of only limited interest and utility. Discussion of U.S. domestic security structures and their coordination may help illustrate the challenges faced by democracies, particularly by illustrating how external actors are able to exploit gaps within the U.S. system.

Approaches to consider:

- Discussion of intelligence coordination reform and challenges since 9/11.
- Concept of gray area operations, as articulated particularly by Joint Special Operations Command.
- Discussion of the U.S. Department of Defense concept of irregular warfare.
- Discussion of the U.S. concept of political warfare.

#### Learning Method/Assessment

Lecture and discussion led by a U.S. SME on U.S. internal security organizations and challenges.

Lecture and discussion on U.S. doctrine for gray area and irregular warfare.

Discussion of problems associated with drawing a sharp distinction between irregular warfare and conventional warfare, particularly regarding resources and activity coordination.

## References

The White House, National Security Strategy, October 2022, <https://www.whitehouse.gov/wp-content/uploads/2022/11/8-November-Combined-PDF-for-Upload.pdf>.

The White House, National Security Strategy of the United States, December 2017, <https://history.defense.gov/Portals/70/Documents/nss/NSS2017.pdf?ver=CnFwURrw09pJ0q5EogFpwg%3d%3d>.

U.S. Department of Defense, National Defense Strategy of the United States, January 2018, <https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf>.

Joint Chiefs of Staff, Description of the National Military Strategy of the United States, 2018, <https://history.defense.gov/Portals/70/Documents/nms/NMS2018%20Overview.pdf?ver=oERVYfgg1p-jtKkYsZHQ%3d%3d>.

Department of Homeland Security, The DHS Strategic Plan, Fiscal Years 2020-2024, [https://www.dhs.gov/sites/default/files/publications/19\\_0702\\_plcy\\_dhs-strategic-plan-fy20-24.pdf](https://www.dhs.gov/sites/default/files/publications/19_0702_plcy_dhs-strategic-plan-fy20-24.pdf).

U.S. Army Training and Doctrine Command (TRADOC), The Operational Environment 2021-2030: Great Power Competition, Crisis, and Conflict, April 2021, <https://oe.tradoc.army.mil/2021/10/04/the-operational-environment-2021-2030-great-power-competition-crisis-and-conflict-2/>.

## T3-B2: China

### Description

China is the world's largest country by population and fourth largest in area. Unlike the United States' democracy, China's political system is based on the autocratic leadership of the Chinese Communist Party, which has about 90 million members. Although the PRC appears unitary, the country suffers from diffuse centers of regional power. Further, given its economic and industrial rise since about 1980, China has progressively asserted itself and expanded its external sphere of influence. This new assertiveness includes activities such as the Belt and Road Initiative, island-building in the South China Sea, development of advanced and extensive cyber tools and weapons, and the persistent theft of intellectual property. The PRC also exercises many methods associated with hybrid threat vectors to include elite capture, economic penetration (e.g., purchasing strategic land holdings), intimidating its diaspora communities, detaining foreign nationals for business disputes, planting agents of influence, gaining dominant positions in international bodies, using lawfare (e.g., through Interpol Red Notices) to harass critics, building extensive fishing fleets and its maritime militia/Coast Guard to squat on contested regions, funding various media outlets and labor groups, and employing transnational criminal gangs to further its external agenda. In 1999, China developed one of the earliest modern expressions of hybrid warfare: "Unrestricted Warfare." The construct of unrestricted warfare has been amplified by additional PRC asymmetrical warfare concepts such as "Three Warfares." This block will explore these concepts and related activities.

### Background

Today's China is still deeply influenced by the long historical and intellectual legacies of its 5,000-year-old civilization. Its current military and political thought have foundations in classical military writing such as *The Art of War*, but also remain influenced by models advanced by Confucius and others. Politically, a strong legacy of grievance remains from the 19th century "open door" policy when Great Britain, France, Germany, Japan, and the United States had a strong military and diplomatic presence within China, which included British engagement in the Opium Wars and suppression of the Boxer Rebellion. China fell into a protracted civil war in the 20th century and was then invaded by Japan in 1936 and occupied until 1945. The long struggle between Chinese Nationalist forces (the KMT) and the Chinese Communist Party



(CCP)/People's Liberation Army (PLA), ended only in 1949 with the KMT retreating to the island of Taiwan. PRC sources refer to this period (1839-1949) as "the century of humiliation" and its legacy remains a strong motivating factor behind Chinese foreign and military policy.

For three decades after 1949, China concerned itself primarily with internal strife and its immediate periphery. The PRC intervened on the Korean peninsula in 1950, fought border wars with India and Vietnam, and on occasion had border clashes with Russia. Following its failure to force Vietnamese troops out of Cambodia in 1979 and fueled by its tremendous economic growth since about 1980, China has become more vociferous in claiming what it considers to be traditional territories and undertaken a major expansion of its military capabilities to reinforce those claims.

The CCP came to power through a combination of political warfare, guerrilla warfare, and conventional warfare. The concept of People's War articulated by Chairman Mao Zedong helped mobilize all facets of society in the struggle against Japan and the KMT. People's War was much more than large-scale guerrilla warfare; indeed, the final campaigns were large-scale battles waged by conventional military organizations. Following the PLA's poor showing in its war with Vietnam, however, the Chinese military embarked on an effort to harness modern technology for military purposes. Since the early 1990s, when the fruits of technological and operational overmatch were demonstrated during the first Gulf War, the People's War has integrated conventional warfare concepts with insurgent and political warfare practices and a whole-of-nation approach to strategy. Some of these efforts will be explored in relation to hybrid threats and hybrid warfare with Chinese characteristics.

### Learning Outcomes

Students will be able to:

- 1) Understand the evolution of Chinese military doctrine from People's War and Protracted War through Unrestricted Warfare and Three Warfares.
- 2) Demonstrate familiarity with China's concepts of strategy, methods, and organization for external influence outside standard economic and diplomatic channels, and the use of its maritime militia and Coast Guard as adjuncts to its rapidly expanding Navy in local and regional intimidation and coercion.
- 3) Understand the elements of China's State-Party interactions on political, economic, military, and technological issues.
- 4) Demonstrate an understanding of China's military and security organs, including the police and militias.
- 5) Understand the debate surrounding China's Belt and Road Initiative (BRI). Participants should understand the purposes of BRI, how it serves Chinese military and political-economic interests, and how it is perceived by international actors.

### Issues for Potential Modules and Approaches to Consider

China's National Defence in the New Era:

- International military competition is undergoing historic changes posed by China's rapid military growth and modernization—these developments warrant detailed attention.
- New and high-tech military technologies based on IT are developing rapidly.
- A prevailing trend exists to develop long-range precision, intelligent, stealthy or unmanned weaponry and equipment.
- Reform in China's military leadership and command system represents a significant measure toward answering the call for a modern, specialized military capable of fighting and winning wars in the information age.
- Military and State security apparatuses for domestic, regional and international influence.
- The United Front approach: coordination among Intelligence, security services, the PLA, and diaspora communities.
- Geopolitical designs, particularly in the South China Sea.
- Use of fishing fleet and maritime militia in neighboring state or contested waters.
- The presence of Chinese police stations in foreign nations.

## Learning Method/Assessment

SMEs will have to decide the depth of exposure to historical material on China that their students need. Forms of teaching and assessment should be appropriate to the depth required.

Given China's global reach, students should be exposed to at least a passing discussion of the Chinese concepts of Civil-Military Fusion and the strategies of indirection and undermining of will suggested by classic Chinese military thinkers.

## References

- Kerry Brown, *China's Dream: The Culture of Chinese Communism and the Secret Sources of Its Power* (Cambridge, UK: Polity, 2018).
- Bernard D. Cole, *China's Quest for Great Power: Ships, Oil, and Foreign Policy* (Annapolis, MD: U.S. Naval Institute Press, 2016).
- Rush Doshi, *The Long Game: China's Grand Strategy to Displace American Order* (Oxford: Oxford University Press, 2021).
- China: The Three Warfares, May 2013, [https://www.esd.whs.mil/Portals/54/Documents/FOID/Reading%20Room/Litigation\\_Release/Litigation%20Release%20-%20China-%20The%20Three%20Warfares%20%20201305.pdf](https://www.esd.whs.mil/Portals/54/Documents/FOID/Reading%20Room/Litigation_Release/Litigation%20Release%20-%20China-%20The%20Three%20Warfares%20%20201305.pdf).
- Frank Hoffman, "Examining Complex Forms of Conflict: Gray Zone and Hybrid Challenges," PRISM 7, no. 4 (November 8, 2018), <https://cco.ndu.edu/News/Article/1680696/examining-complex-forms-of-conflict-gray-zone-and-hybrid-challenges/>.
- Elsa Kania, "The PLA's Latest Strategic Thinking on the Three Warfares," China Brief, Jamestown Foundation 16, no. 13 (August 2016), <https://jamestown.org/program/the-plas-latest-strategic-thinking-on-the-three-warfares/>.
- Sulmaan Wasif Khan, *Haunted by Chaos: China's Grand Strategy from Mao Zedong to Xi Jinping* (Cambridge, MA: Harvard University Press, 2018).
- Sangkuk Lee, "China's 'Three Warfares': Origins, Applications, and Organizations," Journal of Strategic Studies 37, no. 2 (April 2014): 198–220.
- Peter Mattis, "China's 'Three Warfares' in Perspective." War on the Rocks, January 30, 2018, <https://warontherocks.com/2018/01/chinas-three-warfares-perspective/>.
- Orville Schell and John Delury, *Wealth and Power: China's Long March to the Twenty-First Century* (New York: Random House, 2013).
- Andrew Scobell, Edmund J. Burke, and Cortez A. Cooper, *China's Grand Strategy: Trends, Trajectories, and Long-Term Competition* (Santa Monica, CA: RAND Corporation, 2020).
- John P. Sullivan, "Chinese Overseas Police," Iris Report, October 28, 2022, [www.iris.report/p/chinese-overseas-police](http://www.iris.report/p/chinese-overseas-police).
- John P. Sullivan, "Countering Chinese Overseas Police," Iris Report, November 7, 2022, <https://www.iris.report/p/countering-chinese-overseas-police>.
- Qiao Liang and Wang Xiangsui, *Unrestricted Warfare* (Beijing, CN: PLA Literature and Arts Publishing House, 1999), <http://www.c4i.org/unrestricted.pdf>.
- The Science of Military Strategy (Beijing, CN: PLA Academy of Military Sciences, 2013), available in English through the U.S. Air Force Project Everest, "In Their Own Words: Foreign Military Thought, Science of Military Strategy (2013), <https://www.airuniversity.af.edu/CASI/Display/Article/2485204/plas-science-of-military-strategy-2013/>.

### T3-B3: Russia

#### Description

Even prior to the invasion of Ukraine on February 24, 2022, Russia's actions generated a great deal of interest in hybrid threats and hybrid warfare. Such interest has been particularly strong among the nations immediately on Russia's periphery, including in the Caucasus and Central Asia. Like China, Russia is a significant power, having the world's largest nuclear arsenal and a substantial military and intelligence apparatus; however, Russia also has a fragile economy based on natural resource extraction and an authoritarian semi-presidential political system. Russia has published many articles related to hybrid warfare. Now called "New Generation Warfare" in Russia, hybrid warfare has earlier been labeled as the "Gerasimov Doctrine" of non-linear war or the "Primakov Doctrine" to counter a U.S.-led unipolar world order. Whatever label is applied, Russia has actively used hybrid threats or hybrid warfare in a series of wars and military campaigns, including the two Chechen wars of the 1990s-2000, the Georgian war of 2008, the Ukraine war of 2014-present, the Syrian civil war of 2015-present, and in its intelligence and political operations in many other countries in Europe, North America, Latin America, and Africa. These activities have helped spark an international flurry of interest regarding hybrid threats and hybrid warfare. This block explores some key issues in Russian security and defence writings/doctrine that inform Russian activities.

#### Background

Russia's blend of direct military action, employment of proxy military forces, subversion of local political processes, and corruption of border guards and local police—as well as its denials of participation in the capture of Crimea and in the civil war that occurred in eastern Ukraine in 2014—have helped focus attention on hybrid threats/hybrid warfare. For a while, the combination of these actions was viewed as implementation of the "Gerasimov Doctrine." (The scholar who coined that term, however, later averred he was simply putting together a picture of what happened rather than claiming Russia had a fully fleshed out hybrid threat/hybrid warfare doctrine). Subsequently, Chief of the Russian General Staff General Valery Gerasimov, Russia's senior military officer (at least at the time these words were being written), articulated comprehensive guidance on integrating all forms of informational, subversive, diplomatic, and other tools in pursuit of Rus-

sian policy objectives to create a crisis, justify rapid conventional military intervention on Russia's behalf, and then seek a peace agreement or ceasefire to secure Russian gains. (See the brief article by Charles K. Bartles, "Getting Gerasimov Right," *Military Review*, January-February 2016, pp. 30-38). Doing so would entail using all means of dis- and mis-information, political confusion, assassination, espionage, subversion, and coercion, as well as conventional force demonstrations and posturing. All such means were also employable outside the immediate zone of crisis or interest and within both friendly and non-friendly states. Leaders within the Kremlin, particularly former Russian Foreign and Prime Minister Yevgeny Primakov have influenced the comprehensive civil-military campaigns to regain Russia's near abroad, traditional spheres of influence, or many of the borders of the former Soviet Union and to challenge the international order dominated by norms espoused by the United States. These nationalistic and revanchist elements are strong features within the Russian polity—and they are not unique to the current war in Ukraine.

#### Learning Outcomes

Students will be able to:

- 1) Summarize how Russia is striving to regain its place as a dominant actor in regional and global affairs, including the increasing rejection, manipulation, and obfuscation of international norms and practices.
- 2) Understand the kleptocracy and its effects on Russian politics with a specific focus on the relationship between organized crime and the security apparatus and how their ties influence Russia's hybrid warfare methodology.
- 3) Understand the relationship between Russia's military infrastructure and substate/paramilitary actors (e.g., Wagner) in hybrid warfare activities.
- 4) Understand the role deception (*Maskirovka*) plays in Russian hybrid doctrine.
- 5) Explore responses to Russian hybrid warfare and influence operations.

#### Issues for Potential Modules and Approaches to Consider

Depending on the audience, the structures of Russia's state security and defence apparatuses warrant examination in some detail. Local SMEs should strive to outline the specific structures comprising the various Russian

organizations that engage in hybrid threat/hybrid warfare activities. Some threats may need to be addressed at a classified level.

Force multipliers—such as the role of Russian state media, the leadership of the Russian Orthodox Church, and organized crime—should also be examined:

- Russian organized crime is well integrated into the Russian political and economic establishments.
- Explore the role of corruption, oligarchs, and organized crime (Vory)—specifically the use of transnational organized crime and illicit economic flows (e.g., London economic hub).
- Energy, food, natural resources, and their combination with influence operations are also worth studying.

### Learning Method/Assessment

Lectures, analysis of historical and current military theory, review of secondary literature, and case studies.

### References

- Daniel P. Bagge, *Unmasking Maskirovka: Russia's Cyber Influence Operations* (New York: Defense Press, 2019).
- Manuel Castells and Emma Kiselyova, «Russia and the Network Society: An Analytical Exploration,» conference paper presented at Stanford University, November 5-7, 1998, <https://web.stanford.edu/group/Russia20/volume/pdf/castells.pdf>.
- Samuel Charap et al., *Russian Grand Strategy: Rhetoric and Reality* (Santa Monica, CA: RAND Corporation, 2021).
- Brandon A. Davis, «Holy War: How Putin Weaponized the Russian Orthodox Church,» unpublished Master's thesis, Naval Postgraduate School, September 2019, <http://hdl.handle.net/10945/63444>.
- Gregory L. Freeze, «Russian Orthodoxy and Politics in the Putin Era,» Task Force on U.S. Policy Toward Russia, Ukraine, and Eurasia, Carnegie Endowment for International Peace, February 9, 2017, <https://carnegieendowment.org/2017/02/09/russian-orthodoxy-and-politics-in-putin-era-pub-67959>.
- Mark Galeotti, *The Vory: Russia's Supper Mafia* (New Haven: Yale University Press, 2018).
- Mark Galeotti, «Gangster's Paradise: How Organized Crime Took over Russia,» *The Guardian*, March 23, 2018, <https://www.theguardian.com/news/2018/mar/23/how-organised-crime-took-over-russia-vory-super-mafia>.
- Misha Glenny, *McMafia: A Journey Through the Global Criminal Underworld* (New York: Vintage Books, 2009).
- Ian Kelly and David J. Kramer, «Ukraine Isn't the Only Target of Putin's Aggression,» *The Bulwark*, February 22, 2022, <https://www.thebulwark.com/ukraine-isnt-only-target-putins-aggression/>.
- Taras Kuzio, *Russian Nationalism and the Russian-Ukrainian War: Autocracy-Orthodoxy-Nationality* (London: Routledge, 2022).
- David Masci, «Split Between Ukrainian, Russian Churches Shows Political Importance of Orthodox Christianity,» Pew Research Center, January 14, 2019, <https://www.pewresearch.org/fact-tank/2019/01/14/split-between-ukrainian-russian-churches-shows-political-importance-of-orthodox-christianity/>.
- Michael McFaul, «Defending U.S. Allies and Interests Against Russian Aggression in Eastern Europe,» Testimony before the Subcommittee on National Security of the Committee on Oversight and Reform, U.S. House of Representatives, 117th Congress, February 16, 2022, <https://michaelfaul.com/articles/defending-us-allies-and-interests-against-russian-aggression-eastern-europe>.
- Ben Ryan, «Putin and the Orthodox Church: How His Faith Shapes His Politics,» *Theos*, February 16, 2022, <https://www.theosthinktank.co.uk/comment/2022/02/16/essay-on-vladimir-putin>.
- Eugene Rumer, «The Primakov (Not Gerasimov) Doctrine in Action,» Carnegie Endowment for International Peace, June 5, 2019, <https://carnegieendowment.org/2019/06/05/primakov-not-gerasimov-doctrine-in-action-pub-79254>.
- Louise Shelley, «A Tangled Web: Organized Crime and Oligarchy in Putin's Russia,» *War on the Rocks*, November 15, 2018, <https://warontherocks.com/2018/11/a-tangled-web-organized-crime-and-oligarchy-in-putins-russia/>.
- The National Security Strategy of the Russian Federation, July 2021, Текст правового акта в ИПС «Законодательство России» • Официальный интернет-портал правовой информации, [pravo.gov.ru](http://pravo.gov.ru).



### T3-B4: Regional Powers

#### Description

Against the backdrop of renewed great power competition with hybrid threat and hybrid warfare characteristics, regional powers have separate and distinct challenges. All states may be subjected to hybrid threat/hybrid warfare methods, and they may use these methods themselves. We have not supplied a comprehensive list of what might be termed “regional powers” here; however, states such as the United Kingdom and France, which exercise a global presence and have considerable military capacities, would be seen as regional powers. Similarly, India is a major economic power and has a robust military capacity, including nuclear weapons. Pakistan and North Korea also have nuclear weapons and powerful militaries. Iran is a major regional power capable of sustaining numerous active political-military campaigns outside its borders. This list obviously could be expanded.

This block should address the security challenges, response architecture, and national perspective on such issues for countries that the course designers decide are appropriate for examination.

#### Learning Outcomes

Students will be able to:

- 1) Identify, assess, and categorize the geopolitical capabilities of select states outside the major global powers.
- 2) Understand how regional powers are affected by hybrid threats/hybrid warfare waged by state and nonstate actors in a fluid international order.
- 3) Understand how regional powers engage great powers and nonstate actors to achieve geopolitical aims.
- 4) Examine how regional states innovate to project their capacity and geographic reach.
- 5) Understand how regional powers may use hybrid threats/hybrid warfare to advance their ability to influence events beyond their regional reach.

#### Issues for Potential Modules and Approaches to Consider

Local SMEs should lead a discussion on how to identify, assess, and categorize states that could be described as regional powers and may be of interest or concern to the students.

Local SMEs should identify national experts and engage with their government elements that deal with hybrid threats/hybrid warfare to develop this discussion. Identifying roles, missions, and national political positions should be included to address challenging security and defence questions.

#### Learning Method/Assessment

See previous examples.

#### References

Local SMEs will need to determine with which countries they want their students to gain familiarity. The SMEs should then develop suitable sources that address the relevant questions on organizations and capabilities of concern. Some recommended resources on the United Kingdom and France are:

Global Britain in a Competitive Age: The Integrated Review of Security, Defence, Development and Foreign Policy, presented to Parliament by the Prime Minister, March 2021, [www.gov.uk/official](http://www.gov.uk/official) documents.

“Defence – 2021 strategic renewal/summary – Communiqué issued by Mme Florence Parly, Minister for the Armed Forces (Paris, 22 Jan. 21),” France Diplomacy, Ministère de l’Europe et des Affaires Étrangères, January 26, 2021, <https://www.diplomatie.gouv.fr/en/french-foreign-policy/security-disarmament-and-non-proliferation/news/article/defence-2021-strategic-renewal-summary-communique-issued-by-mme-florence-parly>.

### T3-B5: Small States

#### Description

Small states find themselves in unique geopolitical circumstances influenced by history, geography, and other factors. Since the resources of small states are usually limited, they are vulnerable to hybrid attack. In some instances, however, a more centralized governance structure allows small states to focus their resources on particular threats. Further, small states may take part in regional security alliances for collective defence and security. Such alliances increasingly play a crucial role in limiting the impact of hybrid threats and warfare. Some countries using this curriculum may be in this category. This block presents an opportunity for such states to discuss their national situation, threats, and challenges, and to evaluate the security and defence organizations that are responsible for addressing such threats. Response efforts can be addressed under Theme 4.

#### Learning Outcomes

Students will be able to:

- 1) Assess the unique challenges faced by small states in their ability to identify, engage, and prevent hybrid threats/hybrid warfare.
- 2) Describe ways that small powers can compensate for their limited defensive capacities.
- 3) Assess the capabilities of smaller states to project power through hybrid threats/hybrid warfare.
- 4) Understand the broader relationships that smaller powers establish with regional and global powers.

#### Learning Method/Assessment

National Case Studies

#### References

Alyson J.K. Bailes, "Small States and Security: Does Size Still Matter?" chapter 2 in *Small States in the Modern World: Vulnerabilities and Opportunities*, eds. Harald Baldersheim and Michael Keating (Northampton, MA: Edward Elgar Publishing, 2015), 23–41, <https://doi.org/10.4337/9781784711443>.

Christopher Browning, "Small, Smart and Salient? Rethinking Identity in the Small States Literature," *Cambridge Review of International Affairs* 19, no. 4 (2006) 669–84, <https://doi.org/10.1080/09557570601003536>.

Murat Caliskan, "Hybrid Warfare Through the Lens of Strategic Theory," *Defense & Security Analysis* 35, no. 1 (2019) 40–58, <https://doi.org/10.1080/14751798.2019.1565364>.

Håkan Edström, Dennis Gyllensporre, and Jacob Westberg, *Military Strategy of Small States: Responding to External Shocks of the 21st Century* (London: Routledge, 2018).

Mark Ellul, "A Changing Security Environment and Hybrid Threats: The Use of Shelter Theory in Maltese Security," Master's thesis, Charles University, Faculty of Social Sciences, Institute of Political Science, Department of Security Studies, 2022, <https://dspace.cuni.cz/bitstream/handle/20.500.11956/174433/120417506.pdf?sequence=1>

Caroline Kennedy-Pipe and Iftikhar Zaidi, "The Hybrid Challenge and Small States," in *Small States and the New Security Environment*, eds. Anne-Marie Brady and Baldur Thorhallsson (Cham, SZ: Springer International Publishing, 2021), 27–39, <https://doi.org/10.1007/978-3-030-51529-4>.

Robert Keohane, "Lilliputians' Dilemmas: Small States in International Politics," *International Organization* 23, no. 2 (1969) 291–310, <https://www.jstor.org/stable/2706027>.

Heidi Maurer, "When 'Small' Translates as a Lack of Vision and Action," *The Institute of International & European Affairs*, 2020, <https://www.iiea.com/sdses/heidimaurer/>.

Ali Naseer Mohamed, "The Diplomacy of Micro-states," *Netherlands Institute of International Relations "Clingendael"*, <http://www.jstor.org/stable/resrep05362>.

### T3-B6: Nonstate Actors – NGOs and Cities

#### Description

As hybrid threats and hybrid warfare actions aim to influence through coercion and other means, nonstate actors may become vehicles or targets of such activities. Prime among these nonstate actors are elements of civil society. This block focuses discussion on two elements: nongovernmental organizations (NGOs) and cities.

NGOs and various civil society organizations have grown exponentially in number during the past four decades. Along with their raw numbers, their influence on global, regional, and local matters is also increasing. Their activities have become more visible, and their potential value to other actors attracts attention to their existence and activities. Both Russia and China have banned many western NGOs from working within their territories. In conflicts, NGOs have become both actors and targets.

NGOs can be willing participants in a hybrid operation, but they can also be coerced or duped into playing a role desired by the hybrid actor. They can also be purposefully created to be used as channels to wash money and exert influence on a foreign society as part of a wider influence operation. One example is the role of the Russian Orthodox Church in Putin's hybrid-political warfare approach. Others include the host of organizations that the PRC's United Front office supports within Chinese expatriate communities.

Finally, this block draws attention to the role of cities as an increasingly relevant vector in hybrid threat/hybrid warfare. In recent decades, cities have become major economic, political, social, and cultural hubs in an increasingly integrated global economy. They have become international actors through increased police diplomacy and international cooperative agreements. As such, they can be focal points of hybrid threat activities. Global cities, such as Rio De Janeiro, Los Angeles, Hong Kong, London, and New York, are particularly important in understanding the nature of hybrid threats in a global age. The city of Los Angeles, for instance, has more known gang members than there were Viet Cong in South Vietnam. New York was once a major center for financing the Irish Republican Army. Toronto once served as a major financial hub and R&R destination for the Tamil Tigers. The city of Helsinki, Finland, has produced a report on the city as a target for hybrid threats, which can serve as a basis for discussion of other urban centers.

#### Learning Outcomes

Students will be able to:

- 1) Show familiarity with several NGOs banned within Russia and China, and the role of Russian and Chinese NGOs operating internationally.
- 2) Explain the Helsinki city report and apply its findings to a city identified by the course SMEs.

#### Issues for Potential Modules and Approaches to Consider

- Terrorist safe havens and finance centers.
- Organized crime and civil disobedience.
- Targeting of mixed loyalty and diaspora communities.
- Money laundering, informal banking, and remittance cultures.

#### Learning Method/Assessment

- Lecture and discussion.
- Case studies.

#### References

- Joana Gomes Beirao, "The Role of Non-governmental Organizations in International Economic Law," *Lawyr.it*, 6, no. 2 (June 2019), <https://lawyr.it>
- Brandon A. Davis, «Holy War: How Putin Weaponized the Russian Orthodox Church,» unpublished Master's thesis, Naval Postgraduate School, September 2019, <http://hdl.handle.net/10945/63444>.
- Gregory L. Freeze, «Russian Orthodoxy and Politics in the Putin Era,» Task Force on U.S. Policy Toward Russia, Ukraine, and Eurasia, Carnegie Endowment for International Peace, February 9, 2017, <https://carnegieendowment.org/2017/02/09/russian-orthodoxy-and-politics-in-putin-era-pub-67959>.
- Taras Kuzio, *Russian Nationalism and the Russian-Ukrainian War: Autocracy-Orthodoxy-Nationality* (London: Routledge, 2022).
- David Lewis, "Non-governmental Organizations, Definition and History," in *International Encyclopedia of Civil Society* (New York: Springer, 2010), 1056-62.
- Johnathan Manthorpe, *Claws of the Panda: Beijing's Campaign of Influence and Intimidation in Canada* (Toronto: Cormorant Books, 2019).

David Masci, «Split Between Ukrainian, Russian Churches Shows Political Importance of Orthodox Christianity,” Pew Research Center, January 14, 2019, <https://www.pewresearch.org/fact-tank/2019/01/14/split-between-ukrainian-russian-churches-shows-political-importance-of-orthodox-christianity/>.

Massimo Pani, “Countering Hybrid Threats in Megacities and Densely Populated Urban Areas,” in NATO Science for Peace and Security Series, Volume 140, Countering Terrorism and Urban Warfare (Amsterdam, NL: IOS Press, 2018), 71-75.

Ben Ryan, «Putin and the Orthodox Church: How His Faith Shapes His Politics,” Theos, February 16, 2022, <https://www.theosthinktank.co.uk/comment/2022/02/16/essay-on-vladimir-putin>.

Sarah Stroup, “NGOs and States in Global Politics: A Brief Review,” E-International Relations, August 2020, <https://www.e-ir.info/2020/08/03/ngos-and-states-in-global-politics-a-brief-review>.

Peter Willetts, Non-Governmental Organizations in World Politics: The Construction of Global Governance (London: Routledge, 2011).

“Helsinki in the Era of Hybrid Threats – Hybrid Influencing and the City,” (Helsinki, FI: Central Administration Publishing, 2018), [https://www.hel.fi/static/kanslia/Julkaisut/2018/hybridiraportti\\_eng\\_020818\\_netti.pdf](https://www.hel.fi/static/kanslia/Julkaisut/2018/hybridiraportti_eng_020818_netti.pdf).

“Russia: History of NGOS Named as ‘Foreign Agents,”” Civic Solidarity, [www.civicsolidarity.org](http://www.civicsolidarity.org).

### **T3-B7: Criminal Networks, Mercenaries, Corporations, and Other Proxy Actors**

#### **Description**

Some nonstate actors have unique characteristics that allow them to directly compete with and influence states. Definitional boundaries between these actors are elastic. These actors can play more than one role, and they include corporations; private military and security companies (PMCs/PSCs); criminal armed groups (CAGs), gangs, and militias; and transnational criminal organizations (TCOs).

Globalization has provided added scale and capability to enable these proxy actors to influence regional, national, and global environments, working independently or collaboratively with each other or with states aimed at influencing institutions and individuals and influencing state and individual behaviors.

In all cases, tracing networks is key to understanding the success and utility of proxy actors. These networks can be dark (illicit), light (legitimate), or gray (a mixture), and they can be critical components of a hybrid campaign.

TCOs rely on illicit flows which are critical to their operation (money laundering or trafficking in drugs, people, wildlife, ivory, gemstones, avocados, and weapons, etc.) The relationship between the states and these networks typically results in corruption, collusion, and in extreme cases, state capture and reconfiguration.

According to Manuel Castells, “The Perverse Connection: The Global Criminal Economy,” chapter 3 in *End of Millennium, The Information Age: Economy, Society and Culture Vol. III* (Oxford: Blackwell, 2000), 192:

This crime-penetrated business linked up with politicians at the local, provincial, and national levels, so that, ultimately, the three spheres (politics, business, crime) became intertwined. It does not mean that crime controls politics or that most businesses are criminal. It means, nonetheless, that business operates in an environment deeply penetrated by crime; that business needs the protection of political power; and that many politicians, in the 1990s, have amassed considerable fortunes through their business contacts.



Transnational private military organizations also have grown in number dramatically during the past 30 years, and their relationships with private financial interests and legitimate state actors may not always be acknowledged or known. Russia has clearly shown that it is prepared to engage such entities to wage its external military campaigns. Many NATO members have also employed such forces. The role of such elements in hybrid threats and hybrid warfare must be considered.

### Learning Outcomes

Students will be able to:

- 1) Distinguish several types of proxy actors directly engaged in hybrid threats/hybrid warfare.
- 2) Demonstrate an understanding of the multifaceted and complex relationships that can exist between different state and nonstate actors, including those actors who are not geographically proximate to each other.
- 3) Understand and trace the connections between dark (illicit), light (legitimate) and gray (a mixture) networks.
- 4) Demonstrate some familiarity with the nexus of organized crime and social unrest or disobedience in one of the major cities identified in T3-B6 (Non-state Actors—NGOs and Cities) or one selected by local SMEs.

### Issues for Potential Modules and Approaches to Consider

- The role of corporations – particularly their engagement of PMCs for local security.
- Vulnerabilities that criminal networks can exploit.
- Organized crime – present a picture germane to the students.
- Transnational illicit financial flows and methods of facilitation.

### Learning Method/Assessment

- Case studies of network actors.
- Tactical decision game showing networks, their capabilities, and their vulnerabilities.
- Tactical decision game on information sharing related to illicit criminal networks.

### References

Marina Caparini, “Transnational Organized Crime: A Threat to Global Public Goods,” Commentary/Backgrounders, Stockholm International Peace Research Institute, September 2, 2022, <https://www.sipri.org/commentary/topical-Backgrounder/2022/transnational-organized-crime-threat-global-public-goods>.

Luis Jorge Garay, Eduardo Salcedo-Albarán, and Isaac De León-Beltrán, “From State Capture towards the Co-opted State Reconfiguration,” SSRN Electronic Journal, May 2009 (Series at ResearchGate), [https://www.researchgate.net/publication/256012836\\_From\\_State\\_Capture\\_towards\\_the\\_Co-opted\\_State\\_Reconfiguration\\_An\\_Analytical\\_Synthesis](https://www.researchgate.net/publication/256012836_From_State_Capture_towards_the_Co-opted_State_Reconfiguration_An_Analytical_Synthesis).

Nils Gilman, Jesse Goldhammer, and Steven Weber, eds., *Deviant Globalization: Black Market Economy in the 21st Century* (New York: Continuum, 2011).

Adam Isacson, “Great-Power Competition Comes for Latin America,” *War on the Rocks*, February 24, 2022, <https://warontherocks.com/2022/02/great-power-competition-comes-for-latin-america/>.

Frank Madsen, *Transnational Organized Crime* (London: Routledge, 2009).

John P. Sullivan, “How Illicit Networks Influence Sovereignty,” chapter 10 in *Convergence: Illicit Networks and National Security in the Age of Globalization*, eds. Michael Miklaucis and Jacqueline Brewer (Washington, DC: National Defense University Press, 2013).

Charles Tilly, “War Making and State-Making as Organized Crime,” in *Bringing the State Back In*, eds. Peter Evans, Dietrich Rueschemeyer, and Theda Skocpol (Cambridge, UK: Cambridge University Press, 1985), 169–91.

As well, the extensive literature on private military corporations should be explored.

### **T3-B8: Multinational Organizations – EU, NATO, and UN**

#### **Description**

Although security and defence studies tend to see state and nonstate actors as the primary agents and targets of hybrid threats and hybrid warfare, international organizations can also be targets of malign attacks either as direct targets or through attacks on member states. However, crucial differences in the governance structure, membership, and scope of these organizations should be recognized to understand the nature of the threats and respective responses. This block also draws attention to the challenges of coordination at an international level, and the challenge of balancing the organizational aims with the national interests of member states. Local SMEs will have to determine how much and what aspects of this discussion are germane to their students.

#### **Background**

The nature of the European Union (EU) is unique, being distinguished from other international organizations as the only supranational entity in existence. Under its complex and extensive treaty structure, member states have ceded large parts of their sovereign decision-making to the institutions of the Union, such as the Commission and the European Court of Justice. A significant percentage of domestic laws and regulations within the member states come directly from the EU institutions. Although the EU works under the principle of shared sovereignty, complementarity, and subsidiarity (that is, the right of local communities to make decisions for themselves, including the decision to surrender decision-making to a larger forum), states retain powers to set their security policies. This shared sovereignty between supranational and national institutions is perceived as inhibiting a unified central response to hybrid threats and hybrid warfare. Various institutions within the EU, such as the Commission and the Council, have their own agencies, high-level expert groups, and task forces that deal with tracking and evaluation/risk assessment of emerging hybrid threats. Furthermore, the individual member states pursue their own solutions, which are often not integrated into the various EU responses. Finally, different constitutive elements of what are understood to be hybrid threats and warfare are treated separately. For example, the High Representative for Foreign Affairs launched the East StratCom Task Force in response to a disinformation case in 2015, whereas the Commission formed a High-Level Expert Group on Fake News.

The EU recognizes that responding to hybrid threats is a national issue but aims to support its partners and to coordinate actions with both member states and NATO. Its emphasis is on growing societal, economic, and political resiliency at the national and EU level; however, EU members still perceive that it lacks a top-level political commitment to responding seriously to these threats.

NATO has invested in its ability to prepare for, deter and defend against the full spectrum of hybrid threats. It has expanded its tool box while recognising that primary responsibility for responding to hybrid attacks lies with the targeted nation. NATO has adopted an actor specific approach to countering hybrid threats by developing tailored comprehensive (civil and military) preventive and responses options for Allies to consider in countering specific threats. Tools include a deployable Counter Hybrid Support Team, consultations under Article 4 of the Washington Treaty and military activities all of which aim to pose strategic dilemmas for potential adversaries. NATO doctrine highlights that hybrid operations against the Alliance could reach the level of an armed attack and could lead to the invocation of Article 5 by the North Atlantic Council. NATO cooperates closely with partners and with the European Union.

The governance structures of international organizations and alliances provide potential targets for hybrid operations. For example, malign actors seeking to stall a unified response have actively courted high-ranking officials in various European governments and thereby have played a useful role in thwarting concerted action by the EU or NATO. Although member states have their own national interests, successfully countering a hybrid operation may require stronger central control or unified action.

The challenges faced by the EU and NATO are also evident in the governance and decision-making mechanisms of the UN. The UN response to hybrid threats and hybrid warfare is further limited by a set of unique challenges. As the only international organization with near-universal membership and without geographic limits, the UN is tasked with the maintenance of international peace and security — a rather broad and undefined area of operations. Moreover, many potential hybrid threat actors are also its members. At the same time, the UN Charter provides a minimal security role for the organization, one that is further curtailed by the veto power of the five permanent members of the UN Security Council. In practice, the mandates and structure of UN peace-

keeping operations must now include some mechanisms to counter hybrid threats and actors, such as police forces with military units to address nontraditional sources of threats to peacebuilding. The UN refers to these as complex emergencies — the same term used in reference to international peace and security challenges.

The issues discussed above present themselves in other international organizations that engage in multilateral cooperation. Multilateral organizations depend on consensus among member states, which at times can be challenging to achieve, resulting in delays or inaction thus leaving some issues unresolved. Hybrid threat actors leverage and exploit such rifts to undermine the performance of international multilateral organizations.

### **Learning Outcomes**

Students will be able to:

- 1) Show familiarity with several types of international organizations and be able to identify the crucial distinguishing attributes and challenges of multilateralism.
  - 2) Understand how the transnational and supranational nature of the EU (especially the complex relationship between the supranational and national elements of the EU) and the subsidiarity—those elements member states have allowed the EU to assume powers for—and complementarity and cooperative principles influence the kinds of responses the EU can make to hybrid threats and hybrid warfare.
  - 3) Understand the historical and geographical context within which NATO operates and which determine its membership, zone of influence, and scope of operations, to gauge the nature of the hybrid threats and warfare directed against the alliance.
  - 4) Understand the post-Second World War security architecture embodied in the UN Security Council and the limited role it can play in maintaining international peace and security with renewed great power competition.
- The impact of the Russia-Ukraine War on NATO's operation and activities, and NATO's reinvigorated role.
  - Approaches and practices of non-European security organizations may be explored.

### **Issues for Potential Modules and Approaches to Consider**

- EU's security governance model and its weaknesses.
- NATO–EU cooperation on security issues, especially opportunities and challenges.
- The impact of hybrid threats on traditional UN peacekeeping operations.

## Learning Method/Assessment

- Lectures, case analyses, and study of institutional archives and policy output.
- Scenario-based exercise.
- Tactical decision-making exercise on multi-agency task force creation and management.
- Tabletop exercise (TTX) including multi-domain actors from the broad range of subject matter experts required to combat hybrid threats.

## References

Eitvydas Bajarūnas, «Addressing Hybrid Threats: Priorities for the EU in 2020 and Beyond,» European View, March 22, 2020.

Jakub Janda, «EU Response to Pro-Kremlin Propaganda Needs a Change of Pace,» Hybrid and Transnational Threats, Friends of Europe, Winter 2018.

D.A. Kerigan-Kyrou, “The EU & NATO: Promoting Collaboration Between Two of the World’s Most Powerful Organizations,” *Concordiam: Journal of European Security and Defense Issues* 6, no. 3 (September 11, 2015): 16-21, <https://perconcordiam.com/the-eu-nato/>.

Alan Milward, *The European Rescue of the Nation State* (Oakland, CA: University of California Press, 1992).

European Commission and High Representative of the Union for Foreign Affairs and Security Policy, Joint Framework on Countering Hybrid Threats: A European Union Response, Joint Communication to the European Parliament and the Council, June 4, 2016, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016JC0018#:~:text=This%20Joint%20Communication%20aims%20to%20facilitate%20a%20holistic,that%20may%20also%20contribute%20to%20countering%20hybrid%20threats.>

European Commission and High Representative of the Union for Foreign Affairs and Security Policy, Report on the Implementation of the 2016 Joint Framework on Countering Hybrid Threats and the 2018 Joint Communication on Increasing Resilience and Bolstering Capabilities to Address Hybrid Threats, May 29, 2019, [https://www.ecas.europa.eu/node/63378\\_en](https://www.ecas.europa.eu/node/63378_en).

Council of the European Union, A Strategic Compass for Security and Defence – For a European Union That Protects Its Citizens, Values and Interests and Contributes to International Peace and Security, March 21, 2022, <https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/en/pdf>.

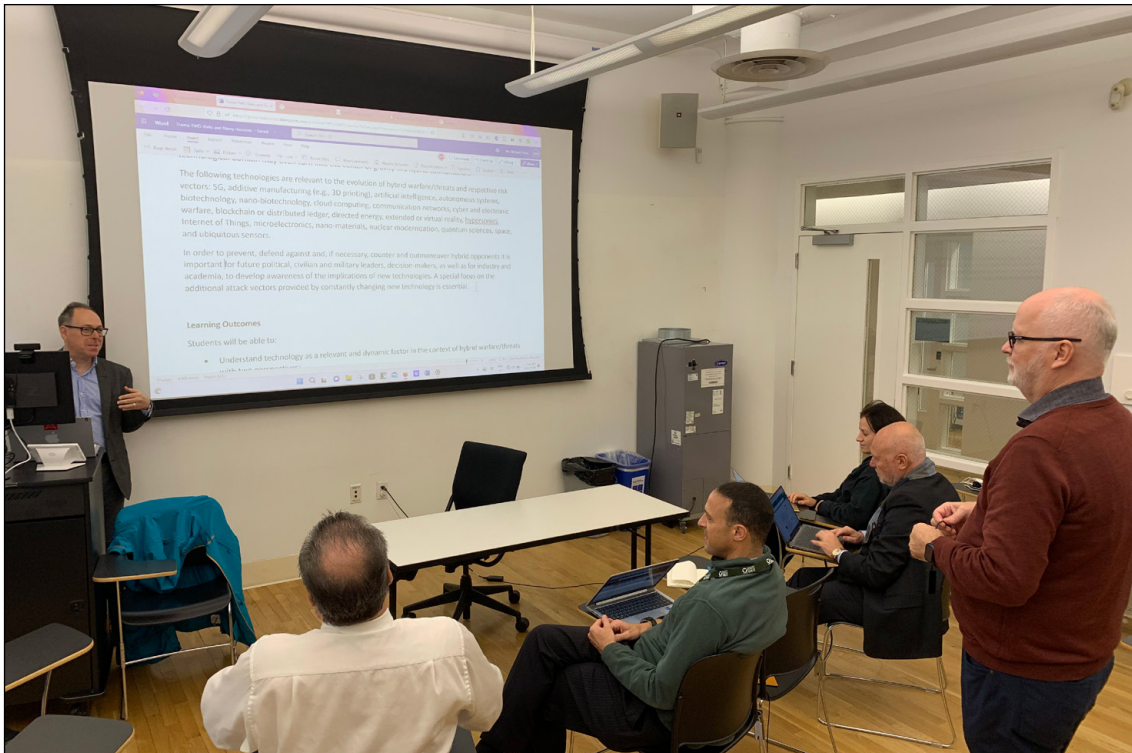
The NATO Stability Policing Center of Excellence (NATO SP COE), <https://www.nspcoe.org>

Hybrid Center of Excellence (HybridCoE)

European External Action Service

Dag Hammarskjöld Library ([research.un.org](https://research.un.org))





Hybrid Threats and Hybrid Warfare Reference Curriculum Writing Team Workshop, Garmisch-Partenkirchen, February 2022.



Hybrid Threats and Hybrid Warfare Reference Curriculum Writing Team Workshop, Garmisch-Partenkirchen, February 2022.





## Theme 4 – Countering Hybrid Warfare and Hybrid Threats

### Goal

NATO's Strategic Concept of 2022 calls for members to "prepare for, deter, and defend against the coercive use of political, economic, energy, information and other hybrid tactics by state and non-state actors." We explore numerous measures suggested or taken to counter such activities and threats. Although there are several individual measures, there is also a logic to conceiving a whole-of-government and whole-of-society approach instead of more narrow approaches. But there is no single solution as many measures require careful calibration in democratic societies and may be constrained by the rule of law and constitutional concerns, among others. A number of passive measures, from awareness building to resilience training, are explored but it warrants note that even a defensive posture may require active steps beyond a defensive defense. Just as nations have come to realize that cybersecurity may require taking the initiative beyond national boundaries similar efforts may be the most effective counters to hybrid threats and malign campaigns.

### Description

The wide range of malign activities subsumed within hybrid threats or hybrid war poses challenges to defenders and target country populations. Forms of openly hostile behavior by external actors or proxies are the most recognizable because of their visibility and tendency to unite societies (e.g., rally around the flag). More indirect activities or long-term subversive activities, such as media influence campaigns (e.g., external ownership, monies and advertising, and disinformation) or buying political influence, are harder to recognize as emanating from a hostile external state agent. This block explores approaches for responding to these security challenges.

### Background

Both state and nonstate actors have many methods open to them to undermine the national will and societal cohesion, confuse observers, obfuscate actions, and pursue Goals through overt and covert actions. All societies have divisions such as an urban/rural divide, linguistic or ethnic distinctions, and religious or other affinity groupings that can be exploited.

As addressed in prior themes, liberal democratic political systems offer disparate interests' vehicles to find accommodation within the polity and representation through the electoral process. Hybrid actors aim to build legitimacy within target governments and exploit and undermine the population's trust in the institutions. Western democracies have focused on ensuring civil and international peace, peaceful resolution of conflicts, maintenance of the social order, and good representative governance. Further national legal and constitutional and international norms—such as the UN's Universal Declaration of Human Rights—promise to protect minorities and pluralistic societies. Additionally, globalization—considered here as the free movement of people, monies, goods, and information—offers interdependencies and efficiencies but also offers hybrid threat actors the chance to create or exploit dependencies and vulnerabilities.

Legal and transparent internal political activity is a feature of modern Western state systems. While a foreign power may seek to influence or subvert the political and socioeconomic order one must recognize that local political interests may apply such a label to delegitimize their political opponents. It may be difficult to disentangle the legitimate from the illegitimate. With this in mind, several activities to counter such threats are explored. Whole-of-government and whole-of-society efforts may be simple solutions to extol but much more challenging to execute in response to the complexity of various hybrid threats and activities.

### Learning Outcomes

Students will be able to:

- 1) Describe the complexity of the strategic context in which hybrid tactics and countermeasures are used.
- 2) Discuss how a local population is a center of gravity when hybrid tactics are being used.
- 3) Recognize the need for whole-of-government and whole-of-society approaches to information sharing, situational awareness, coordination, and collaboration.

## Suggested References

Beyond the sources listed under each block see:

Catherine Belton, *Putin's People: How the KGB Took Back Russia and then Took on the West* (UK: HarperCollins, 2021).

Mason Clark, *Russian Hybrid Warfare* (Washington, D.C.: Institute for the Study of War, 2020), <https://understandingwar.org/report/russian-hybrid-warfare>.

Heather A. Conley, James Mina, Ruslan Stefanov, and Martin Vladimirov, *The Kremlin Playbook: Understanding Russian Influence in Central and Eastern Europe* (Washington, D.C.: CSIS, 2016), <https://csd.bg/publications/publication/the-kremlin-playbook-understanding-russian-influence-in-central-and-eastern-europe/>

Patrick J. Cullen and Erik Reichborn-Kjennerud, "Understanding Hybrid Warfare," A Multinational Capability Development Campaign project (MCDC, 2017), [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/647776/dar\\_mcdc\\_hybrid\\_warfare.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/647776/dar_mcdc_hybrid_warfare.pdf).

Oleksandr V. Danylyuk, *Interagency and International Cooperation in Detection and Countering Hybrid Threats* (Kyiv: Center for Defense Reforms, 2021).

Frank Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars* (Arlington, Virginia: Potomac Institute for Policy Studies, 2007), <https://potomacinstitute.org/reports/19-reports/1163-conflict-in-the-21st-century-the-rise-of-hybrid-wars>.

Vytautas Keršanskas, "Deterrence: Proposing a More Strategic Approach to Countering Hybrid Threats," HYBRID CoE Paper 2. March 2020. [note graphic model proposed herein would be a useful teaching tool. We should ask for permission to reproduce.]

Guillaume Lasconjarias and Jeffrey A. Larson, eds., "NATO's Response to Hybrid Threats," NATO Defence College Forum Paper 24, (NDC, 2015).

Michael Miller, *Hybrid Warfare: Preparing for Future Conflict* (Maxwell AFB AL: Air War College, 2015), <https://apps.dtic.mil/sti/citations/ADA618902>.

Lyle J. Morris, Michael Mazarr, Jeffrey Hornung, Stephanie Pezard, Anika Binnendijk, and Marta Kepe. *Gaining Competitive Advantage in the Gray Zone: Response Options for Coercive Aggression Below the Threshold of Major War*. RAND Corporation, 2019. <https://doi.org/10.7249/RR2942>.

Mikael Weissmann; Nilsson, Niklas; Thunholm, Per & Palmertz, Bjorn. eds., *Hybrid Warfare: Security and Asymmetric Conflict in International Relations* (London: I.B. Taurus, 2021).

James Whiter, "Making Sense of Hybrid Warfare," *Connections: The Quarterly Journal* 15, no. 2 (2016): 73-87, <https://doi.org/10.11610/Connections.15.2.06>.



## T4-B1: Frameworks and Strategies to Counter Hybrid Threats

### Description

This block surveys conceptual frameworks and strategies to counter hybrid threats and warfare. Given the range of threat actions, it is suggested that comprehensive whole-of-society response frameworks be instituted to mitigate, prevent, protect, respond, and deter overt and covert hybrid warfare operations. However, this may be difficult, if not impossible, to achieve in multi-party, pluralistic democracies

A comprehensive framework may not exist within a country adopting this reference curriculum. It is unsafe to assume that all necessary domestic governments and civil society stakeholders are now involved. Therefore, local subject matter experts and representatives from nongovernmental organizations (NGOs) and private sector entities should be engaged through formal and informal activities, with government leaders who can speak to teamed national and societal efforts to counter a broad range of hybrid threat activity.

This block also examines response frameworks that suggest a full range of recommended measures regarding information sharing and collaboration between governmental, private, and civil society actors. Additionally, this block should include information on where participants can find suggested policies, draft procedures, and potential national architectures, for responding to hybrid threats and hybrid warfare.

### Learning Outcomes

Students will be able to:

- 1) Analyze frameworks, concepts, and strategies to prepare for, deter, and protect against hybrid threats and related fields (e.g., cybersecurity, transnational organized crime, critical infrastructure protection, terrorism, and counter-corruption).
- 2) Understand and explain the security architecture of their home country and its involvement in multilateral, international, and supranational organizations.
- 3) Recognize how malign actors analyze the architecture of a target country to attack vulnerable areas where policies or competencies are unclear, insufficient, or overlapping.
- 4) Understand the role of NGOs and private sector entities in domestic security architecture.

### Issues for potential modules and approaches to consider.

- Escalation of response measures.
- Collaboration boundaries and limits between government institutions and their division of labor.
- Overcoming new challenges with existing infrastructure allows opponents to exploit preexisting societal challenges.
- Role of civil society and domestic or international NGO entities (e.g., third-party watchdog groups or international monitoring groups).
- Various legal frameworks (e.g., domestic, transnational, international). Understanding the differences between home country domestic law, treaty law, laws of armed conflict (IHL/LOAC), human rights law (IHRL), and international norms frequently referred to by NATO members and partner states.
- Nonviolent resistance concepts and best practices in interpersonal relationships to counter malign actors acting to foment or accelerate societal divisions. Examples may include grassroots communication to create community resilience, such as a periodic gathering of local leaders (e.g., police chiefs, NGOs, labor organizers, private sector entities, religious leaders, and other stakeholders) to build trusted cross-sector relationships.
- Countering adversary misinformation and disinformation and the role of civil society concerning information operations.

### Learning Method/Assessment

- Subject Matter Experts (SME) presentations on domestic security architecture.
- Tabletop exercises (e.g., wargaming) to build an understanding of possible domestic reactions to hybrid attacks, identify gaps, and design practical responses. (Include government, NGO, and other public SME representation)

## References

Mohamed S. Helal, "On Coercion in International Law," *International Law and Politics*, Vol. 52:1, 26 Dec. 2019, pp. 1-122. <https://www.nyujilp.org/wp-content/uploads/2020/01/NYI101.pdf>

Michael Rühle and Clare Roberts, "Enlarging NATO's Toolbox to Counter Hybrid Threats," *NATO Review*, March 19, 2021, <https://www.nato.int/docu/review/articles/2021/03/19/enlarging-natos-toolbox-to-counter-hybrid-threats/index.html>.

V. Stoian, Policy integration across multiple dimensions: The European response to hybrid warfare, *Studia Politica* 19(3-4), 2019, pp. 97-126.

Tim Sweijts; Zilincik, Samuel; Bekkers, Frank & Meessen, Rick. A Framework for Cross-Domain Strategies Against Hybrid Threats, The Hague Centre for Strategic Studies, 2021, <https://hcss.nl/news/new-report-a-framework-for-cross-domain-strategies-against-hybrid-threats/>

Dick Zandee, Sico van der Meer, and Adája Stoetman, Countering hybrid threats (Clingendael: Netherlands Institute of International Relations, 2021), <https://www.clingendael.org/pub/2021/countering-hybrid-threats/>.

COE (Finland) Framework (see above).

EU policy for countering hybrid threats, <https://ccdcoe.org/incyder-articles/eu-policy-on-fighting-hybrid-threats/>.

"Detect-Deter-Respond" in Countering Hybrid Warfare, MCDC (2019). "Why Information Matters: A Foundation for Resilience," *Internews Center for Innovation & Learning*, 2015. <https://internews.org/resource/why-information-matters-foundation-resilience/>

Albert Einstein Institution, "198 ways of nonviolent action," (2014 & 2017), <https://www.brandeis.edu/peace-conflict/pdfs/198-methods-non-violent-action.pdf>

## T4-B2: The Role of the Military in Response to Hybrid Threats and Hybrid Warfare

### Description

This block surveys the military's role in responding to hybrid threats and warfare. The focus is on the roles and responsibilities of state militaries in dealing with domestic and international threats. It is expected that local SME will develop this discussion in light of national authorities and jurisdictions.

This block explores the advantages and disadvantages of military response to nonmilitary attacks. It examines the legal authorities to act domestically and internationally in response to such threats while considering international military cooperation and coordination.

The domestic discussion should include elements of a state's security apparatus charged with overseeing, coordinating, or contributing to the response mission.

### Learning Outcomes

Students will be able to:

- 1) Understand the role of the military in hybrid warfare nonmilitary operations.
- 2) Explain local factors in coordinating military actions with other institutions.
- 3) Recognize how malign actors target defense capabilities in hybrid operations.
- 4) Discuss the ROEs kinetic and non-kinetic responses
- 5) Discuss military mitigation responses to hybrid operations.
- 6) Understand response option escalation in hybrid warfare domains (e.g., kinetic to non-kinetic means, humanitarian factors, and the laws of armed conflict).
- 7) Discuss challenges regarding attribution and response escalation using military resources in hybrid operations.

### Issues for potential modules and approaches to consider.

Possible questions to explore:

- Stages of escalation in response? How are responsibilities divided in own country? Are there overlaps, or conflicting competencies?

- Roles of actors in consequence management and potential new tasks for the military? The leading role, supporting role?
- Describe the escalation of hybrid threats, appropriate responses within a country, national authorities & legal frameworks, commercial sector roles, and responsibilities.
- Identify the conditions for triggering NATO's Article 5.
- Describe the military's role and infrastructure for information sharing (e.g., plans & triggers for levels of sharing/declassification).
- Define and describe institutional/transnational trust frameworks.

### Learning Method/Assessment

- SME presentations on domestic security architecture and the place of the military in domestic security.
- Case studies on the involvement of the military in countering hybrid threats. Seminar discussions with government and nongovernment representation to gain insight into the respective infrastructure and processes.
- Table-top exercises to gain insights into possible domestic reactions to hybrid attacks, identify gaps and design practical responses.

### References

Local SMEs should spend considerable effort finding the national level guidance and policies and key stakeholders who may supply learning resources.

Todor Tagarev, "Reflecting Developments in Hybrid Warfare into Defence Policy," in *Countering Hybrid Threats: Lessons Learned from Ukraine*, edited by Niculae Iancu, Andrei Fortuna, Cristian Barna, Mihaela Teodor (Amsterdam: IOS Press, 2016): 27-33, <https://doi.org/10.3233/978-1-61499-651-4-27>.

Mikael Weissmann, "Conceptualizing and countering hybrid threats and hybrid warfare: The role of the military in the grey zone," in *Hybrid Warfare: Security and Asymmetric Conflict in International Relations*, edited by Mikael Weissmann, Niklas Nilsson, Björn Palmertz, and Per Thunholm (London: I.B. Tauris, 2021), 61–82, <https://doi.org/10.5040/9781788317795.0011>.

For a collection of European Union statements and reports see <https://euhybnet.eu/other-publications/>

For a collection of publications and case studies see the site of the Hybrid CoE, <https://www.hybridcoe.fi/publications-and-readings/>

On the role of military instruments in deterrence. See, Hague Center Strategic Studies, <https://hcss.nl/news/new-report-a-framework-for-cross-domain-strategies-against-hybrid-threats/>

## T4-B3: Nonmilitary Approaches and Means for Countering Hybrid Threats

### Description

This block explores nonmilitary approaches to counter hybrid threats through public and private organizations. While some approaches are sector-specific, cross-sector information sharing is important to maintain situational awareness. There is a logic to seek a single coordination center to ensure a common operating language and team mitigation efforts –but for various reasons states may avoid creating such an organization.

### Learning Outcomes

Students will be able to:

- 1) Recognize different societal sectors that are involved in countering hybrid threats.
- 2) Explain the advantages of collaborative responses to hybrid threats.
- 3) Explain the limitations of individual sector approaches to countering hybrid threats.
- 4) Recognize the need for both regulatory and nonregulatory approaches to counter hybrid threats across societal sectors.

### Issues for potential modules and approaches to consider.

- The role of the private sector.
- Sector and organizational approaches and measures.
- Ownership and investment transparency in critical infrastructure owned or operated by the private sector or nonmilitary organizations (e.g., energy, telecom, media/social media, financial services, cryptocurrencies, alternative methods of wealth transfer, etc.).
- Finance transparency of domestic political parties, and local and international civil society organizations and non-governmental organizations.
- Supply chain visibility and vulnerability assessment across sectors.
- Countering malign influence in democratic processes.
- Limiting malign propaganda and opportunities for disinformation.
- Countering malign cyber espionage on the private sector and nonmilitary targets.

- The importance of individual citizen awareness and societal digital literacy.

### Learning Method/Assessment

- Presentation and analysis of case studies from selected sectors.
- Seminar discussions on the limitations of strategies and countermeasures at the individual sectors/organizations.

### References

See all earlier References.

Catherine Belton, *Putin's People: How the KGB Took Back Russia and Then Took on the West* (UK: HarperCollins, 2021).

Heather A. Conley, James Mina, Ruslan Stefanov, and Martin Vladimirov, *The Kremlin Playbook: Understanding Russian Influence in Central and Eastern Europe* (Washington, D.C.: CSIS, 2016), <https://csd.bg/publications/publication/the-kremlin-playbook-understanding-russian-influence-in-central-and-eastern-europe/>

Heather A. Conley, Donatienne Ruy, Ruslan Stefanov, and Martin Vladimirov, *The Kremlin Playbook 2: The Enablers* (Washington, D.C.: CSIS, 2019), <https://www.csis.org/analysis/kremlin-playbook-2-enablers-0>

NATO-EU Joint Framework on countering hybrid threats and related documents at [https://ec.europa.eu/defence-industry-space/hybrid-threats\\_en](https://ec.europa.eu/defence-industry-space/hybrid-threats_en)

See resources at European Centre for Countering Hybrid Threats, (Helsinki), <https://www.hybridcoe.fi/hybrid-threats/>



## T4-B4: Information Collection, Analysis, and Sharing

### Description

This block examines how to collect, analyze, and share information for foresight and early warning unique to hybrid threats and hybrid warfare. A major early warning challenge is to identify a coordinated hybrid influence or threat campaign or the development of such tools in support of hybrid competition or conflict. There is the challenge of amplifying weak signals that may portend coordination and cooperation across layers and forms of government (i.e., recognizing an attack and getting an agreed understanding of such an attack may prove a major challenge before an effort at countering the effort may be made). The theory and practice of strategic foresight across the whole of government should be examined.

While it can begin with a general discussion, it is important to focus discussion on national organizations, roles, missions, and practices. Internal state security practices, organizations, and legal frameworks share many similarities across nations, but all are nevertheless unique. Participants need to understand the unique structures, roles, missions, authorities, and the issues of intelligence production on on Hybrid Threats and Hybrid Warfare.

National SMEs need to elaborate on specific national practices. It is worth noting that some states are becoming dependent on external, third-party private contractors for Open-Source intelligence (OSINT). OSINT techniques may be used by states and those in service to states, helping to uncover, collect, and analyze information. OSINT can also include social media intelligence (SOCMINT) that may be crowdsourced. These actors may themselves fall victim to hybrid techniques or may have complicated allegiances.

Discussion should then raise the questions of who puts together a 'whole picture' and then how holistic policies are generated. If there is a national fusion center its structure and role should be discussed; alternative structures for sharing may also be addressed. Collection of intelligence may occur across a wide spectrum, but analysis benefits from centralization and sharing. Discussion should include legal reviews, interagency responses, and building doctrine to fill the gaps. Inter-alia discussion may turn to 'gap' management, and relations between civilian, police, and military security services. As well, there should be a discussion of securing and maintaining (i.e. probative chain of custody) evidence for use in the legal system and courts.



Figure 2. The Intelligence Cycle

## Learning Outcomes

Students will be able to:

- 1) Describe how the intelligence cycle applies to local situational awareness and coordination.
- 2) Describe the role of information-sharing agreements for situational awareness and response coordination to hybrid threats.
- 3) Describe the impact of diverse organizational cultures and the need for trust in both cross-sector and transnational information sharing.

## Issues for potential modules and approaches to consider.

- Information and intelligence support requirements.
- Information sharing arrangements case studies (e.g., counterterrorism and cybersecurity purposes).
- Advantages and disadvantages of information sharing arrangements across domestic sectors and for transnational purposes.
- Needs and opportunities for dissemination of intelligence products nationally and internationally.
- Risks and opportunities of using open-source intelligence.
- The structure, roles, and authorities of national and local intelligence agencies and organizations

## Learning Method/Assessment

- Presentation and analysis of case studies from national and sectoral experience.
- Seminar discussions on the intelligence cycle at individual sectors/ organizations based on advantages and disadvantages.
- Scenario-based exercises involving all information gathering and sharing entities (see T2-B7)

## References

Bespoke list by local SMEs.

National-level policies and laws should be used as primary sources.

Emma Van Goethem and Marleen Easton, “Public-Private Partnerships for Information Sharing in the Security Sector: What’s in It for Me?” *Information & Security: An International Journal* 48, no. 1 (2021): 21-35, <https://doi.org/10.11610/isij.4809>.

NATO Intelligence, Surveillance, and Reconnaissance in the Baltic Region ([jstor.org](https://www.jstor.org/stable/2765444))

NCI Agency | Joint Intelligence, Surveillance and Reconnaissance ([nato.int](https://www.nato.int))

## T4-B5: Coordination and Collaboration in Countering Hybrid Threats

### Description

The purpose of this block is to emphasize the importance of and explore frameworks, procedures, and organizations to ensure effective coordination and collaboration among stakeholders in implementing strategies (Block 1) for countering hybrid threats.

This block examines national and international collaboration, as well as public-private coordination and the involvement of nongovernmental actors across multiple domains, for instance in the media.

### Learning Outcomes

- 1) Participants understand the roles of other actors and crisis action centers necessary for coordinating (domestic/transnational institutions, companies, etc.)
- 2) Participants understand that inherent gaps are future leverage points that may/not be clear. Such gaps must be addressed in assigning roles and responsibilities.
- 3) Understand the applicability of the concepts, values, and challenges of collaborative information sharing, e.g., Security Operations Centre (SOC) used in the cyber domain or fusion analysis centers in intelligence.
- 4) Understand the importance of national organizational and cultural structures.
- 5) Participants understand the security architecture of their home country and its involvement in multilateral, international, and supranational organizations.
- 6) Develop a deep understanding of the tasks, competencies, and relationships of home national institutions to identify strengths and weaknesses of present institutional arrangements.

### Issues for potential modules and approaches to consider.

- Good practices in interagency coordination and collaboration.
- Good practices in public-private collaboration.
- Good practices and challenges in international collaboration.
- Gap analysis for roles and responsibilities in national arrangements and architectures.

- Collaboration in institutional/legal context.
- Collaboration in cultural context.

### Learning Method/Assessment

- Presentation and analysis of case studies from selected nations and organizations.
- Presentation and analysis of case studies selected from Security Operation Centers (SOCs), e.g., cyber and counterterrorism domains.
- Seminar discussions on the limitations of coordinating countermeasures at the national/international level
- Scenario-based exercises (see T2-B7)

### References

Iztok Prezelj and Joe Airey, "Interagency Cooperation in Counter-Terrorism," in James Wither and Sam Mullins, eds., *Combating Transnational Terrorism* (Sofia: Procon, 2016), 235-252.

Todor Tagarev, "Towards the Design of a Collaborative Cybersecurity Networked Organisation: Identification and Prioritisation of Governance Needs and Objectives," *Future Internet* 12, no 4 (2020), 62, <https://doi.org/10.3390/fi12040062>.

NATO-EU Joint Framework on countering hybrid threats and related documents at [https://ec.europa.eu/defence-industry-space/hybrid-threats\\_en](https://ec.europa.eu/defence-industry-space/hybrid-threats_en)

See resources at European Centre for Countering Hybrid Threats, (Helsinki), <https://www.hybridcoe.fi/hybrid-threats/>

EU programmes (Horizon-2020/ Horizon Europe) investing in R&D and collaboration. See EU-HYBNET links: <https://euhybnet.eu>

The Hague Center for Strategic Studies, A Horizon Scan of Trends and Developments in Hybrid Conflicts set to shape 2020 and beyond, <https://hcss.nl/news/new-publication-a-horizon-scan-of-trends-and-developments-in-hybrid-conflicts-set-to-shape-2020-and-beyond/>



## **T4-B6: Scenarios, Wargaming, and Table-Top Exercises (TTX)**

### **Description**

This block will instruct participants on how to conduct hybrid threat training exercises. Participants will develop an understanding of the value of applying learning methods to a national context. SMEs should explain the utility and design of scenario analysis and wargaming for rehearsing complex response activities.

### **Learning Outcomes**

Students will be able to:

- 1) Understand how to design/select training methods and scenarios.
- 2) Understand how to select and tailor training objectives for specific audiences.

### **Learning Method/Assessment**

- Presentation and analysis of case studies from selected nations and organizations.
- Presentation and analysis of case studies selected from Security Operation Centers (SOC) (e.g., cyber and counterterrorism domains).

- Seminar discussions on the limitations of coordinating countermeasures at the national/international level
- Scenario-based exercises, including Red Team exercises.

### **References**

George Sharkov, Christina Todorova, Georgi Koykov, and Georgi Zahariev, “Hybrid Exercising for Cyber-resilient Healthcare and Cross-sector Crisis Response Operability,” CEUR Workshop Proceedings, 2933 (2021), pp. 329-351, <http://ceur-ws.org/Vol-2933/paper32.pdf>.

Fight Club International Home | UK Fight Club

NATO Wargaming Initiative <https://www.act.nato.int/articles/wargaming-initiative-nato-2022>

PACE–[EU/NATO] Parallel and Coordinated Exercise EU INTEGRATED RESOLVE 2022 EU IR22: Parallel And Coordinated Exercises(PACE) | EEAS Website ([europa.eu](http://europa.eu))

US Army Red Team Handbook [https://usacac.army.mil/sites/default/files/documents/ufmcs/The\\_Red\\_Team\\_Handbook.pdf](https://usacac.army.mil/sites/default/files/documents/ufmcs/The_Red_Team_Handbook.pdf)

## T4-B7: Resilience to Hybrid Threats

### Description

This block explores approaches, methods, and techniques to enhance hybrid threat resilience of individuals, communities, organizations, and societies. Resilience in this context refers to the ability to prepare for, actively resist, and successfully recover from malicious acts associated with hybrid warfare. Physical, technological, and psychological (cognitive-emotional) resilience must be cultivated, amplified, and protected at every level.

### Learning Outcomes

Students will be able to:

- 1) Describe the concept of resilience as it pertains to humans.
- 2) Understand the characteristics of resilience as applied to individuals, communities, organizations, and societies.
- 3) Identify resources for building resilience at each level.
- 4) Analyze existing frameworks and resilience strategies (e.g., national, European Union, and NATO).

### Issues for potential modules and approaches to consider.

- The concept of resilience.
- Possible questions include: Is there an ideal set-up for a nation/society to overcome hybrid threats? Is there a model resilient nation/society? Are there features and characteristics that resilient societies/nations share? How does one instill the will to resist or the will to fight hybrid threats and warfare?
- The need for national resilience and preparedness strategies.

### Learning Method/Assessment

- Case studies from other domains (e.g., climate adaptation, urban planning, cybersecurity, etc.).
- Case studies exploring the concept of resilience and its application to hybrid threats.
- Analysis and presentation of case studies from hybrid warfare and other domains (e.g., crisis/disaster management, cybersecurity, supply chains).
- Seminar discussions on the practical limitations of implementing and assessing the effectiveness of resilience measures.

### References

- Philipp Fluri and Todor Tagarev, "The Concept of Resilience: Security Implications and Implementation Challenges," *Connections: The Quarterly Journal* 19, no. 3 (2020): 5-12, <https://doi.org/10.11610/Connections.19.3.00>.
- Carmit Padan and Reuven Gal, "A Multi-dimensional Matrix for Better Defining and Conceptualizing Resilience," *Connections: The Quarterly Journal* 19, no. 3 (2020): 33-46, <https://doi.org/10.11610/Connections.19.3.02>.
- Peter Rogers, "The Evolution of Resilience," *Connections: The Quarterly Journal* 19, no. 3 (2020): 13-32, <https://doi.org/10.11610/Connections.19.3.01>.
- George Sharkov, "Assessing the Maturity of National Cybersecurity and Resilience," *Connections: The Quarterly Journal* 19, no. 4 (2020): 5-24, <https://doi.org/10.11610/Connections.19.4.01>.
- Björn von Sydow, "Resilience: Planning for Sweden's 'Total Defence'," *NATO Review*, April 4, 2018, <https://www.nato.int/docu/review/articles/2018/04/04/resilience-planning-for-swedens-total-defence/index.html>.
- Nassim Nicholas Taleb, *Antifragile: Things that Gain from Disorder* (London: Penguin, 2013).
- James K. Wither, "Back to the Future? Nordic Total Defence Concepts," *Defence Studies* 20, no. 1 (2020): 61-81, <https://doi.org/10.1080/14702436.2020.1718498>.
- United Nations Office for Disaster Risk Reduction, *Sendai Framework for Disaster Risk Reduction 2015-2030*, <https://www.undrr.org/publication/sendai-framework-disaster-risk-reduction-2015-2030>.

## T4-B8: Recommended Practices from NATO and EU

### Description

In this block, participants will analyze the NATO toolbox and EU policy for countering hybrid threats, (both listed in the References below). Discussion should use these documents as criteria to highlight real-world examples identified by course SMEs. It is recommended that lessons learned and case studies examining successes and failures are prepared.

### Learning Outcomes

Students will be able to:

- 1) Apply lessons learned and case studies.
- 2) Discuss good practices, successes, and failures.
- 3) Analyze the NATO toolbox and EU policy recommendations from the perspective of their home countries.

### Issues for potential modules and approaches to consider.

- Familiarity with the NATO toolbox and EU policy for countering hybrid threats.
- Selecting endogenous case studies that highlight local country challenges.
- Applying lessons learned to home country challenges.

### Learning Method/Assessment

- Presentation and analysis of selected case studies.
- Discuss the application of case studies on hypothetical scenarios.
- Discuss the relevance of policy on operational countermeasures.

### References

Michael Rühle and Clare Roberts, “Enlarging NATO’s Toolbox to Counter Hybrid Threats,” NATO Review, March 19, 2021, <https://www.nato.int/docu/review/articles/2021/03/19/enlarging-natos-toolbox-to-counter-hybrid-threats/index.html>

V. Stoian, Policy integration across multiple dimensions: The European response to hybrid warfare, *Studia Politica* 19(3-4), 2019, pp. 97-126.

Dick Zandee, Sico van der Meer, and Adája Stoetman, Countering hybrid threats (Clingendael: Netherlands Institute of International Relations, 2021), <https://www.clingendael.org/pub/2021/countering-hybrid-threats/>



EU policy for countering hybrid threats, <https://ccdcoe.org/incyder-articles/eu-policy-on-fighting-hybrid-threats/>






## List of Contributors

### Primary Authors, Editors and Project Leads:

Dr. Sean S. Costigan	George C. Marshall European Center for Security Studies	
Dr. Michael A. Hennessy	Royal Military College of Canada	

### Discussion Group Leaders & Main Contributors

Dr. Namrata Goswami	Thunderbird School of Global Management, Arizona State University	
Dr. Everita Silina	The New School University	
Dr. Aleks Nesic	United States Foreign Service Institute	
Dr. Todor Tagarev	Institute of Information and Communication Technologies, Bulgarian Academy of Sciences	

### Significant Contributors




Tornike Asatiani	Georgian Ministry of Defence	
Dr. Dinos Kerigan-Kyrou	NATO Maritime Interdiction Operational Training Centre (NMIOTC)	
COL Soenke Marahrens	European Centre of Excellence for Countering Hybrid Threats	 Hybrid CoE
Dr. Inez Miyamoto	Daniel K. Inouye Asia-Pacific Center for Security Studies	

Dr. Johann Schmid	Center for Military History and Social Sciences of the Bundeswehr (ZMSBw)	
Dr. John P. Sullivan	USC Price Safe Communities Institute, University of Southern California	
LTC Falk Tettweiler	George C. Marshall European Center for Security Studies	
Dr. Marzena Żakowska	War Studies University, Poland	

### Contributors

Anne C. Bader	International Cybersecurity Dialogue LLC	
Simon Bracey Lane	Independent Scholar	
Andrew Borene	United States National Intelligence University	
Chad M. Briggs	Asian Institute of Management	
Nollag Conneely, MSc	Privacy Engine	
Giorgi Dzadzamia	Georgian Ministry of Defence	
LTC Olaf Garlich	Partnership for Peace Consortium	
Michael Gaul	International Board of Auditors, NATO	

Prof. Larry P. Goodson	United States Army War College	
Tamar Gugunishvili	Georgian Ministry of Defence	
Dr. Peter A. Kiss	Hungarian Defence Forces, Force Modernisation and Transformation Command, Scientific Research Centre	
Dr. Elizabeth Kunce-Wagner	Daniel K. Inouye Asia-Pacific Center for Security Studies	
Dr. Niklas Nilsson	Swedish Defense University	
Dr. Aaron Presnall	Jefferson Institute	
Dr. Jean-Marc Rickli	Geneva Centre for Security Policy	
Dr. Carmen Rijnoveanu	Romanian Institute for Political Studies of Defense and Military History	
Clare Roberts	Innovation, Hybrid and Cyber Division, NATO International Staff	
MAJ Martin Schuster	Partnership for Peace Consortium	
COL Vasyi Shkoliarenko	National Defense University of Ukraine	
Dr. Jake Sotiriadis	United States National Intelligence University	

COL (Ret.) Kevin D. Stringer	United States Irregular Warfare Center	
Paul Thurkettle	NATO Allied Command Transformation	
Prof. Mikael Weissmann	Swedish Defense University	



Hybrid Threats and Hybrid Warfare Reference Curriculum Writing Team Workshop, Garmisch-Partenkirchen, February 2022.





#### **Project Lead Authors & Editors**

Dr. Sean S. Costigan  
George C. Marshall European Center for Security Studies  
[sean.costigan@marshallcenter.org](mailto:sean.costigan@marshallcenter.org)

Dr. Michael A. Hennessy  
Royal Military College, Canada  
[Hennessy-m@rmc.ca](mailto:Hennessy-m@rmc.ca)

#### **Layout Coordinator / Distribution**

Gabriella Lurwig-Gendarme  
NATO International Staff  
Defence Education Enhancement Programme (DEEP)  
[lurwig.gabriella@hq.nato.int](mailto:lurwig.gabriella@hq.nato.int)

