Information & Security: An International Journal

Gergana Mitalova, v.39:2, 2018, 127-135 https://doi.org/10.11610/isij.3910

COMPREHENSIVE INSTITUTIONAL APPROACH TO DEVELOPING CAPABILITIES TO COUNTER HYBRID THREATS: LEGAL AND DOCTRINAL LIMITATIONS

Gergana MITALOVA

Abstract: There are few legal instruments addressing the issue of hybrid conflict and threats. Predominantly, they are laid down in international humanitarian law and are overlooked in the states' legal systems. Nowadays, a fully new comprehensive institutional approach to the development of capabilities to counter hybrid threats is needed – an approach at multiple levels, multinational and interdisciplinary, intertwining the achievements known so far with up-to-date innovations.

Keywords: hybrid threats, legal constraints, doctrinal limitations, comprehensive approach, capability development, collaboration, cooperation.

Terminology and Context

The Prussian strategist, Karl von Clausewitz, wrote that one cannot understand war without understanding the broader political and social implications of the context in which it is executed. Any discussion on hybridity, therefore, needs to set the terms in their proper context.

Defining the term 'hybrid threat' is quite controversial itself. According to military studies and publications, there are several interchangeable words, such as:

- hybrid threats
- hybrid war
- hybrid tactics
- ambiguous warfare
- full-spectrum conflict
- unconventional warfare
- non-linear warfare

- asymmetric warfare
- irregular warfare
- grey wars, etc.

The term 'hybrid' has recently been used to capture the seemingly increased complexity of warfare, the multiplicity of parties involved, and the blurred 'traditional' categories of conflict. Hybrid threats can combine conventional military forces—weapons, command and control, and combined arms tactics—something that attributes commonly to guerrilla or criminal organizations. A hybrid threat is a diverse and dynamic combination of regular, irregular forces, and/or criminal elements, which collaborate to achieve mutually benefitting effect. The regular forces are governed by international law, military tradition, and custom. Irregular forces are unregulated and, as a consequence, act with no restrictions on violence. The ability to combine regular and irregular forces and operations makes hybrid threats particularly effective in the pursuit of their objectives.

A persistent obstacle to the understanding of the hybrid threat has been the inability to classify what a 'hybrid threat' is and how it appears. Mainly, the problem is the blank space that exists between the definition and the context in which the hybrid threat emerges. The conclusion is that no definition can be adequate to multiple contexts that differ so much in place and time. So, as there is no universally accepted definition of hybrid warfare, there are often quite visible doctrinal gaps between the different theories.

Some examples could be given in support of the above statements. For instance, in 2008, the US Army Chief of Staff defined a hybrid threat as an adversary that incorporates "diverse and dynamic combinations of conventional, irregular, terrorist and criminal capabilities."

The United States Joint Forces Command defines a hybrid threat as "any adversary that simultaneously and adaptively employs a tailored mix of conventional, irregular, terrorism and criminal means or activities in the operational battle space. Rather than a single entity, a hybrid threat or challenger may be a combination of state and non-state actors."

The U.S. Army defined a hybrid threat in 2011 as "the diverse and dynamic combination of regular forces, irregular forces, criminal elements, or a combination of these forces and elements all unified to achieve mutually benefiting effects."

NATO uses the term to describe "adversaries with the ability to simultaneously employ conventional and non-conventional means adaptively in pursuit of their objectives."

From Terms to Concepts

Generally, hybrid threats are said to seek to exploit the use of media, technology and, frequently, state's political, military, and social infrastructures to their advantage. This explains why hybrid threats are defined as multilevel and diverse, forcing their opponents to react along multiple lines of actions. There are proofs that a 'simple' defence may not provide the resources, intellectual capacity, manoeuvre needed to oppose the hybrid warfare. The reason is that hybrid threats can simultaneously create economic instability, or provoke lack of trust in existing government, and attack information sources and networks, while providing a captivating but destructive message in carrying out their goals. In most cases of enactment, a hybrid threat may result in induced humanitarian or political crisis, or even in a crisis endangering the physical existence of the opponent.

Hybrid threat actions are usually well synchronized and fitted together, so they can take place in various fields at the same time, damaging the information networks, infrastructure, economic and military domains. The war of the new era combines a variety of tools in a wide range of military intelligence capabilities, nonconventional weapons and equipment, as well as a wide-range of criminal activities adding to the hybrid warfare, such as drug smuggling, human trafficking, counterfeiting and piracy.

This clarifies the main difficulty – isolating the specific challenges. There are measures to be taken on one or more of several lines of operations.

Recently, hybrid threats are defined as networks of people, capabilities, and devices that merge, split, and combine in multiple possible ways. Theoretically, each hybrid threat, as well as each participant, provoking it, can be defeated if isolated, and then a proper countermeasure is applied. A typical feature of a hybrid threat is that it prevents its opponents from separating the conflict into easily assailable parts. It is important to note that a military action will be the least important activity involved in a hybrid threat. In no time, the hybrid warfare opponent will already be defeated or at least paralyzed. That is why, adaptation, control of speed, agility, versatility, and changeability are the keys to success in a fight against hybrid warfare opponents, who are adaptive, flexible and widely employing propaganda and various tools for recruiting members.

Traditional military organizations, such as NATO, might find it hard to face a hybrid threat, experiencing a lack of flexibility due to a constant switch to different objectives and priorities. Recently, attempts have been made to craft a process and develop a plan, which is to bring together representatives of all agencies that might participate in such operations, and improve coordination and collaboration between them.

The 2005 National Defence Strategy of the USA defined the modern threats to the West, starting with the traditional ones, analysing the irregular, and concluding with terrorist and disruptive threats. According to this analysis, the new adversaries are supposed to employ all forms of war tactics, mostly simultaneously. Hybrid threats incorporate a full range of modes of warfare, including conventional capabilities, irregular tactics and formations, and terrorist acts.

In the above cited Strategy, there are six principles of hybrid war, defined as follows:

- a hybrid force's composition, capabilities, and effects are unique to the force employment context;
- each hybrid force has a specific ideology that creates an internal narrative to the organization;
- a hybrid force always perceives an existential threat to its survival;
- in hybrid war there is a capability overmatch between adversaries;
- a hybrid force contains both conventional and unconventional components;
- hybrid forces seek to use defensive operations.

To summarise, the future operational environment will be characterized by hybrid threats, and so we need to create a more competitive security environment in order to successfully oppose these threats. No single definition or description could be universally applied, or can be universally relevant to any and all potential hybrid scenarios, as each scenario needs to be fixed in order to fit the gap in the model.

Most references to hybrid war meet the necessity to ensure that the response to a hybrid threat is legitimate and proportionate. The NATO Summit in Wales in 2014 confirmed the application of Article 5 of the Washington Treaty in the event of a cyberattack, but has not established clearly a threshold that would trigger a collective-defence mechanism.

The legal gaps in the hybrid warfare field are even more significant than the doctrinal ones. No international legal framework regulates hybrid warfare. There is a common document where the use of force in international relations is regulated – the United Nations Charter. It states precisely that, in the absence of an armed conflict involving a country or its allies, a member state can use force legally only if authorized by a resolution of the United Nations' Security Council. Other rules and principles regarding armed conflict are laid down in international human rights law and humanitarian law. Analysing hybrid conflict and threats, there is a set of specific legal instruments regarding different objects, such as human rights, counter-terrorism, money laundering and terrorist financing, and cyberspace and seas. At the same time, the boundaries of concepts such as sovereignty, legitimacy and legality are blurred, and new chal-

lenges originate from this complexity, having in mind that the application of international law and the functioning of global governance are harshly diminished.

Towards Enhanced Cooperation in a Comprehensive Framework

To counteract the hybrid threats, a new comprehensive approach is needed by blending all the available instruments: humanitarian aid, political processes, economic development, military force, diplomacy, and rule of law.

Analysing the legal documents on this topic, one can conclude that most of the legal concepts and frameworks do not respond to today's reality. As a result, they do not always address hybrid threats adequately. This leads increasingly to a failure in applying the existing rules correctly and accordingly. Frequently, countries use conventions, bi-lateral, multilateral and international agreements selectively, so that they can justify their positions. The need for new approaches, such as law enforcement, cooperation and mutual legal assistance, concerning the aspect of confronting hybrid threats as a challenge is becoming much more demanding.

To respond to the changes in the security and military sectors, some countries have adjusted to hybrid threats by creating new institutions or by empowering already existing organizations.

Steps in the EU Framework

That is why in April 2016, the EU and its Member States signed a Joint Framework to counter hybrid threats and foster the resilience of the EU, its Member States and partner countries, while increasing cooperation with NATO on countering these threats. Federica Mogherini, the High Representative of the European Union for Foreign Affairs and Security Policy, has stated: "In recent years, the security environment has changed dramatically. We have seen the rise of hybrid threats on EU's borders. There has been a strong call for the EU to adapt and increase its capacities as a security provider. The relationship between internal and external security needs to be further strengthened. With these new proposals, we want to enhance our capacity to counter threats of hybrid nature. In this effort, we will also step up cooperation and coordination with NATO."

Elżbieta Bieńkowska, Commissioner for Internal Market, Industry, Entrepreneurship and SMEs, additionally said: "The EU must become a security provider, able to adapt, anticipate and react to the changing nature of the threats we are facing. This means enhancing our resilience and security from within while increasing our capacity to counter emerging external threats."

Both of them have underlined the importance of applying new legal instruments to the changed socio-political and military situation worldwide, with the everyday presence of hybrid threats.

Basically, the Joint Framework is built on the European Agenda on Security, adopted by the Commission in April 2015, as well as on sectorial strategies, such as EU Cyber Security Strategy, the Energy Security Strategy and the European Union Maritime Security Strategy. As such a combination, the Framework offers a comprehensive approach to improve the common response to the challenges posed by hybrid threats to the collective security of Europe. It unites all relevant subjects to counter and handle hybrid threats in a more precise and refined manner.

The Joint Framework brings together existing policies and proposes twenty-two operational Actions aimed at:

- raising awareness – coordinating EU actions to deliver strategic communication;
- building resilience by insuring cybersecurity, critical infrastructures, namely – Energy, Transport, Space; securing the financial system, public health system and strengthening the security and defence systems;
- in case of a wide-ranging and serious hybrid attack occurrence – preventing, responding to crisis, and recovering by defining effective procedures to follow, but also by examining the applicability and practical implications of the Solidarity Clause (Article 222 TFEU) and the mutual defence clause (Art. 42(7) TEU);
- reinforcing the EU-NATO cooperation in a joint effort to counter hybrid threats, paying respect to the principles of autonomy and inclusiveness of each organization's decision-making process.

The Joint Framework is to provide a sound foundation to support the European countries in countering hybrid threats collectively, supported by a wide range of EU instruments and initiatives and using the full potential of the Treaties.

Hybrid threats refer to a mixture of activities often combining conventional and unconventional methods that can be used in a coordinated manner by state and non-state actors while remaining below the threshold of what can be formally declared as warfare. Their objective is not only to cause direct damage and exploit vulnerabilities, but also to destabilize societies and create ambiguity to hinder decision-making.

While countering hybrid threats is largely a matter of national competence, the primary responsibility lying with the Member States, such threats can be addressed more effectively with a coordinated response at EU level by using EU policies and instru-

ments, to build on European solidarity, mutual assistance and the full potential of the Lisbon Treaty. EU policies and instruments can play a key value-adding role in building awareness and, to a significant degree, they already do. This is helping to improve the resilience of Member States to respond to common threats, paying respect to the principles set out in Article 21 of the Treaty on European Union (TEU) – democracy, the rule and indivisibility of human rights, and respect for the principles of the United Nations Charter and international law, as well as to the principles embodied in the European Defence Action Plan, the EU Cybersecurity Strategy, the Energy Security Strategy, the Aviation Safety Regulation, the Space Surveillance and Tracking Support Framework, the European Programme for Critical Infrastructure Protection, the European Union Maritime Security Strategy and its Action Plan, the European Union Customs Risk Management Strategy and Action Plan, the European Union Agency for Network and Information Security (ENISA), etc.

The EU legal frame has to face the newly appearing challenges – hybrid threat financing, radicalization and violent extremism and terrorism.

In order to do so, the following actions are to be considered: securing the strategic communication, advisory support to the parliament and government; additional border management support in case of emergency. Possibilities of further synergies could be explored among security, customs, and justice actors, including the relevant EU agencies, namely INTERPOL and the European Gendarmerie Force.

An immediate response to events provoked by hybrid threats is required. This could be achieved by using the European Union response mechanisms and early warning systems, precisely including border monitoring, crisis management, protection of high-risk facilities, illicit trafficking export control of dual-use items, first response to emergencies, surveillance and control of deceases, nuclear forensics, post incident recovery, etc. Best practices derived are developed by the European Nuclear Security Training Centre, EUROPOL, FRONTEX, CEPOL, and EUROJUST.

Nowadays, analyses of hybrid threats can be made by the recently established EU Intelligence and Situation Centre (EU INTCEN) of the European External Action Service (EEAS). It can receive, analyse and share classified and open source information, especially relating to indicators and warnings concerning hybrid threats from different stakeholders within the EEAS, including EU Delegations, the European Commission, and the Member States of the European Union.

In collaboration with the existing similar structures at the Union and at national levels, the EU Intelligence and Situation Centre would analyse external aspects of hybrid threats, affecting the EU and its neighbourhood. It is designed to adequately and rapidly analyse relevant incidents and inform the EU strategic decision makers about the

ongoing processes. It will also inform them about the security risk assessments, carried out at the European Union level.

Steps in the NATO Framework

In addition, a profound survey of the NATO related documents is required to get acquainted with the legal frame on combating hybrid threats at international level. One of the most significant legal documents is the 2010 NATO Strategic Concept with its implications on hybrid warfare. It defines several steps of reaction to hybrid threats. The first is to be defined as 'Prevention' – detecting and better understanding of strategic hybrid threats, the already known ones and their modifications; creating a hybrid warfare strategy; creating early indicators to hybrid threats – combining the open and classified resources of information; NATO and the EU working in concert; and building and developing strategic communications. Next is the so called 'adaptation' – envisioning the use of classified and unclassified information alike for adapting the operational training. The last one is to alleviate key vulnerabilities, such as manipulation of the population, influencing the media sources, creating alienation between the social and ethnic groups.

The response to hybrid threats seeks to exploit the connections between collective defence, crisis management and cooperative security. Therefore, there must be created a secured network between the participating actors – states, organizations and individuals, so that they can withstand the hybrid aggression.

That is why NATO Wales Summit had a key role defining the new priorities – a new kind of defence, which is a mixture of advanced deployable forces, cyber security and missile defence. In addition, actions have been outlined to build resilience in areas such as cybersecurity, critical infrastructure, protecting the financial system from illicit use, and efforts to counter hybrid threats.

The implementation of agreed strategies by the EU and the NATO Member States and the total implementation of existing legislation will be a key step, while some more concrete actions are developed and implemented to fill in the legal and doctrinal gaps in the field of the hybrid threats combat.

Once initiated, the effective comprehensive approach will require a unity of effort. Due to the diverse stakeholders, a full unity of command will be hard to achieve. The challenge will not be to define, to identify or put the hybrid threat in a legal frame anymore, but to motivate all the actors – states, governments, NGOs, and civilians, to work together in order to withstand the Twenty first century plague – the hybrid war.

Bibliography

1. Headquarters Department of the Army, "Hybrid Threats," Training Circular, Washington DC, 26 November 2010.
2. Frank G. Hoffman, "Hybrid Warfare and Challenges," *Joint Force Quarterly* 52 (1st Quarter 2009), 34-39.
3. Timothy McCulloh and Richard Johnson, *Hybrid Warfare*, JSOU Report 13-4, (MacDill Air Force Base, FL: The JSOU Press, 2013).
4. Guillaume Lasconjarias and Jeffrey A. Larsen, eds., *NATO Response to Hybrid Threats*, NDC Forum Papers Series (Rome: NATO Defence College, 2015).
5. Julianne Lindley-French, "NATO and the New Ways of Warfare – Defeating Hybrid Threats," Conference Report (Rome: NATO Defence College, April 2015).
6. Michael Aaronson, Sverre Diessen, Yves De Kermabon, Mary Beth Long, and Michael Miklaucicnato, "Countering the Hybrid Threat," *PRISM 2*, no. 4, (September 2011): 111-124.
7. European Commission, "Joint Communication to the European Parliament and the Council: Joint Framework on Countering Hybrid Threats – a European Union response," EUR-Lex - 52017JC0030, 2017.
8. Headquarters Department of the Army, "Meritorious Unit Commendation," no. 2014–64 (Washington, D.C., 26 November 2010).

About the Author

Gergana MITALOVA is a 2012 graduate of the Law Faculty of Sofia University "St. Kliment Ohridski" and a practicing lawyer.