NATO - EU COLLABORATION ON HYBRID THREATS: COOPERATION OUT OF NECESSITY WITH POTENTIAL CONSEQUENCES ON INTERNATIONAL LEGAL FRAMEWORK

Laris Gaiser[*]

Abstract

This article analyzes the current state of collaboration between NATO and the EU, with particular reference to the hybrid conflict sector. There has always existed a close relationship of interdependence between the two organizations. In 2016, this interdependence experienced a collaborative surge with the signing of a joint declaration at the Warsaw Summit. Since then,

[*] **Dr. Laris Gaiser**, ITSTIME. Graduated in Law at the University of Verona in 2002 with a final dissertation on “The consequences of the devolution of power in United Kingdom and the new role of the State in public economy”, earned his Master’s degree in International Affairs and Diplomacy from the Institute for International Political Studies (ISPI) of Milano and, after a specialization in crisis management and humanitarian action at UN Staff College, obtained a Ph.D. in Geopolitical Economy at University Guglielmo Marconi of Rome.From 2012 to 2014 he was Vice President, acting President, of Euro Mediterranean University – EMUNI and member Slovenian Minister of Foreign Affairs’ Strategic Council. Laris Gaiser is president of Slovenian Paneuropean Movement and Presidency member of International Paneuropean Union (Strasbourg). Involved in strategic consultancy, he also served as general manager in several international companies. As a member of ITSTIME – Italian Team for Security, Terroristic Issues and Managing Emergencies - at Catholic University of Milan (Italy), Senior Scholar at Center for the Study of Global Issues at University of Georgia (USA) and Visiting Lecturer at Diplomatic Academy of Vienna, he regularly teaches geopolicy, geoeconomy and intelligence issues.

NATO and the European Union have actively collaborated in various sectors, including hybrid warfare. In the future, both organizations will need to improve the exchange of information and intelligence collaboration. However, this analysis aims to point out that NATO and the EU, if they wish to limit the scope of their opponents' manoeuvrability, since hybrid conflict tends to develop below the threshold of what is generally accepted as the definition of armed conflict, will have to work together to outline a new legal framework that redefines the definition of armed conflict.

Introduction

The antecedent of the European Union, the European Coal and Steel Community, was born just two years after NATO. Since the very beginning, NATO and the European Union have lived in synergy and mutual dependence. Both projects have been shaped in order to deliver security, stability, peace and development to their respective Member States and both are major economic, political and military organizations.

Given that the overwhelming majority of EU members are also members of NATO and given that the EU's enlargement process has at many times followed similar actions by NATO, it is clear that there exist strong strategic and political interactions among them that make both vitally interdependent. Relations between NATO and the EU were institutionalized in 2001, building upon the results of NATO-Western European Union cooperation from the 1990s. The European Union-NATO Declaration on European Security and Defence Policy of 2002 set out the political principles underlying the relationship and reaffirmed assured access of the EU to NATO's planning capabilities for the EU's military operations. Since then, the organizations steadily upgraded their relationship. Close cooperation became an important element in the development of a comprehensive international approach to crisis management and operations, which requires the effective application of both military and civilian means. Based on that understanding, as well as the multiple and ever-evolving contemporary security challenges they faced, NATO and the EU outlined a series of actions in 2016 that the two organizations intend to tackle together in certain areas in order to avoid redundancies in developing a coherent, complementary and interoperable defence capability. Accordingly, countering hybrid threats have been identified as a priority for cooperation.

The scope of this article is to clarify the type of cooperation that NATO and the EU installed in the hybrid warfare field while detecting possible areas for improvement, especially when taking into account that hybrid warfare hardly fits within the currently valid legal framework for regulating armed conflicts.

Definitions

The relative novelty of hybrid warfare lays in the ability of an actor to synchronize multiple instruments of power simultaneously and intentionally exploit the creativity, ambiguity, non-linearity and the cognitive elements of warfare. Hybrid warfare – conducted by state or non-state actors – is typically tailored to remain below obvious detection and response thresholds, often relying on the speed, volume and ubiquity of digital technology that characterizes the present information age. It concludes that hybrid warfare is already prevalent and widespread, is used by state and non-state actors, and is likely to grow as a challenge, justifying new efforts by nations to understand the threat it presents (MCDC, 2017).

According to Hagelstam and Narinen (2018), hybrid threats are diverse and ever-changing, the tools used range from fake social media profiles to sophisticated cyber-attacks, all the way to overt use of military force and everything in between. Hybrid influencing tools can be employed individually or in a combination, depending on the nature of the target and the desired outcome. As a necessary consequence, countering hybrid threats must be an equally dynamic and adaptive activity, striving to keep abreast the variations of hybrid influencing, predicting where the emphasis will be next, and which new tools may be employed. Hybrid conflicts involve multi-layered efforts designed to destabilise a functioning state and polarise society. Unlike conventional warfare, the “centre of gravity” in hybrid warfare is the target country’s population.

Hybrid threats are diverse, tailor-made to exploit specific vulnerabilities of specific targets. This means that each country must have its own strategy directed against it by thoroughly familiarising itself with its own vulnerabilities. Consequently, it is unlikely that a watertight definition of what constitutes a hybrid threat will be formed. However, an accepted shared understanding of the term is needed in order to represent the lowest common denominator of any further regular engagement within and between the relevant EU and NATO structures. In 2010, the NATO Military Working Group (Strategic Planning & Concepts) approved the following definition: “a hybrid threat is one posed by any current or potential adversary, including state, non-state and terrorists, with the ability, whether demonstrated or likely, to simultaneously employ conventional and non-conventional means adaptively, in pursuit of their objectives”(Ventre 2016, 240). However, NATO Strategic Concept 2010 approved a slightly modified definition, according to which hybrid threats are “those posed by adversaries, with the ability to simultaneously employ conventional and non-conventional means adaptively in pursuit of their objectives.” By not specifying state adversaries the definition acknowledges both the ambiguity of the enemy, as well as the simultaneous and combined conventional and unconventional nature of the threat itself.

On the other side, according to European Union documents, hybrid threats combine conventional and unconventional, military and non-military activities that can be used in a coordinated manner by state or non-state actors to achieve specific political objectives. Hybrid campaigns are multidimensional, combining coercive and subversive measures, using both conventional and unconventional tools and tactics. They are designed to be difficult to detect or attribute. These threats target critical vulnerabilities and seek to create confusion, hindering swift and effective decision-making. Hybrid threats can range from cyber-attacks on critical information systems, through the disruption of critical services such as energy supplies or financial services, to the undermining of public trust in government institutions or the deepening of social division (EEAS 2018).

The key to understanding the interest in hybrid warfare within both the EU and NATO, as a challenge that strikes at the core of Western institutional, legal and social foundations, is the Jan Stoltenberg belief that there is a “blurr[ed] line between war and peace”, meaning that there exists “a state which is somewhere in between" (Uzieblo 2017, 13). As Reichborn-Kjennerud and Cullen (2016) critically point out, conflicts no longer follow neat phases, fitting a model which can be used to elaborate appropriate responses, which can lead to interpreting hybrid war as a permanent state of war.

Hybrid warfare, being a fluid security environment, becomes a catalyst for increased EU-NATO cooperation, which carries with it an important symbolic dimension.

Cooperation

According to official EU explanations, its Member States continue to face serious and acute threats, which are increasingly taking non-conventional forms, such as radicalisation leading to terrorist attacks, chemical attacks, cyber-attacks or disinformation campaigns (EEAS 2018). Due to the above reasons, on July 8, 2016, EU and NATO representatives signed a Joint Declaration in Warsaw giving substance to a more concrete partnership. The declaration outlined a set of concrete areas and actions for cooperation with a focus on deliverables. The series of actions the two organizations intend to take together include countering hybrid threats, enhancing resilience, defence capacity building, cyber defence, maritime security, and exercises (NATO 2019).

Consequently, the European Union created the EU Hybrid Fusion Cell to gather information and intelligence from Member States as to inform decision-makers both in EU institutions and Member States, and the European Centre of Excellence for Countering Hybrid Threats in Helsinki to establish a research institution that can provide analysis as well as organize trainings and exercises for EU Member States and NATO Allies. The Centre of Excellence thus could cooperate with all NATO COEs which deal with connected issues feeding into coordinated policy responses for both organisations.

In 2017, the EU and NATO added further areas of joint work for a total of 74 actions. The overwhelming majority of the actions have a long-term perspective requiring continued implementation since they represent recurring processes which continually produce gradual results, rather than single one-off events. However, a process of continuous engagement has been established and, according to the Third progress report on the implementation of the common set of proposals endorsed by NATO and EU Councils, the EU Hybrid Fusion Cell, the NATO Hybrid Analysis Branch and the European Centre of Excellence for Countering Hybrid Threats are all in frequent contact with each other and have developed strong working relationships. On situational awareness, staff-to-staff discussions between respective geographical and thematic clusters of the EU's Single Intelligence Analysis Capacity and NATO's Joint Intelligence and Security Division have been established and the EU Hybrid Fusion Cell and the NATO Hybrid Analysis Branch are also able to communicate via the EU version of the NATO Battlefield Information Collection and Exploitation System (BICES). Furthermore, regular strategic foresight discussions between NATO and EU staff has taken place. The Centre of Excellence effectively contributes to strengthening EU-NATO cooperation in the area of hybrid threats while formulating recommendations for further enhancing cooperation in the fields of early warning and situational awareness, strategic communication and messaging, crisis response, resilience, and cyber defence and energy security (European Council 2018).

Challenges

EU-NATO cooperation, despite numerous historical frictions, is one formed out of necessity, imposed by the international environment, that could have many positive implications. A concrete development of European defence capabilities, avoiding unnecessary redundancies, is key in joint efforts to make the Euro-Atlantic area safer and contribute to transatlantic burden-sharing. In order to improve cooperation in the future, both organizations shall focus on deeper intelligence data exchange, strategic communication, development of coordinated procedures and security capacity building.

Putting aside the various possibilities for technical collaboration, it must be underlined that the European Union is an institution characterized by the principle of mutual defence, while NATO of collective defence, but both organizations face important legal issues in dealing with the new security challenges posed by hybrid threats. Due to their complex nature, and because their inherent operations in the grey area between what is legal and illegal under international law, hybrid threats challenge the need for maximum certainty, a basic assumption underpinning the collective self-defence principle, expressed in Article 5 of the North Atlantic Treaty or the mutual defence principle expressed in Article 42(7) of the Treaty on European Union.

The lack of operational certainty can create unpleasant holes in the Euro-Atlantic security system (European Parliament 2017). For NATO, the notion of deterrence has long been part of its *modus operandi*. This notion seems more complicated as hybrid threats are less *deterrable,* consequently, the idea of deterrence by denial found its place within the Alliance but it is unlikely to succeed given the ambiguity of this new form of warfare (Uzieblo 2017). Therefore, deterrence by resilience became the natural choice in defence planning and the "comprehensive approach" the reference framework for crisis management. A comprehensive approach to crisis management provides political, civilian and military crisis management instruments and requires multiple actors – including from the private sector and NGOs – to contribute a concerted effort, taking their respective strengths, mandates and roles into account.

Shaping interoperable resilience instruments has already achieved positive results within cyber defence cooperation, especially after the signing of the EU-NATO technical arrangement between the NATO Computer Incident Response Capability (NCIRC) and the Computer Emergency Response Team – European Union (CERT-EU) on February 10, 2016 (European Commission 2018). According to NATO's response to hybrid threats document (2018), while the primary responsibility for responding to hybrid threats rests with the targeted nation, NATO is ready, upon Council decision, to assist an ally at any stage of a hybrid campaign. In cases of hybrid warfare, the Council could decide to invoke Article 5 of the Washington Treaty, as in the case of an armed attack. Hybrid threats, however, are characterized by dynamism, complexity and simultaneity and usually take place under the official threshold of what constitutes an armed attack.

Today, they are the manifestation of an inability to fit current security challenges within previously delineated schemata for conceiving war. Given the above, NATO and the EU, in order to narrow the enemies' possibilities for hybrid conflict as well as to clearly define the beginning moment of a state of war, shall soon generally begin to shape and influence the international legal framework. The use of force in international relations is regulated by the United Nations Charter, which states clearly that, in the absence of an armed attack against a country or its allies, a Member State can use force legally only if authorised by a United Nations Security Council resolution, on the other hand, armed conflict is regulated by international humanitarian law and human rights law.

With regard to hybrid conflict and threats, a patchwork of legal instruments covers specific policy areas, the application of existing international law and the functioning of global governance institutions becomes increasingly complicated, the meaning of concepts such as sovereignty, legitimacy and legality are constantly challenged, and in some cases redefined. As Gunneriusson and Ottis (2013) very aptly put it, hybrid threats are not defined by the actors, since states, non-state actors and even individuals might be considered (part of) hybrid threats. It is not about any specific technology since the list here keeps growing as new technologies become available. It is also not about a specific effect, as a hybrid campaign may result in casualties, changed decisions, altered public perception, etc. Perhaps the best way to put it is that a hybrid threat is a manifestation of total war. Consequently, as pointed out already in the field of highly unpredictable cyber conflicts (Gaiser 2017), it is important to understand that adjustments to the existing legal and institutional framework shall be foreseen. They can be achieved only by coordinated efforts of a representative size of the international community of which NATO and the EU are among the most important members.

Changes in the legal interpretation of the definition of armed aggression, or what qualifies a situation to be an armed conflict (Irmakkesen 2014), and whether hybrid conflicts are becoming the future standard for disrupting a society's ability to function (Kramer 2015) will have a long-term impact on the stability of the international order and may eventually result in global power shifts. A common effort in shaping the most appropriate approach toward the review of the international legal order concerning hybrid conflicts could be intended as the deepest development of the comprehensive approach which requires the effective application of both military and civilian means.

Conclusions

The strong and fluid element of ambiguity within hybrid warfare adds a new dimension to how coercion, aggression, conflict and war are to be understood. In this respect, new geostrategic contexts, new applications of technologies, and new organizational forms suggest the likelihood that this form of warfare will persist and continue to evolve into the future (MCDC 2017). The EU and NATO are different organisations. The EU is a political and, in many respects, a supranational entity dealing with a wide range of policies, while NATO is primarily a military alliance. However, both are founded in the same system of values and have major security-related objectives in common.

The two organizations will continue to face common security challenges: this will only reinforce the need for further strengthening of cooperation. Each additional day of cooperation between the EU and NATO, together with the implementation of the EU Global Strategy and the European Defence Action Plan, constitutes an integral pillar of EU's work aimed at strengthening European security and defence, which contributes to Trans-Atlantic burden sharing. Clearly, however, the traditional boundaries defining the conflicts that served as the basis for the Alliance’s historic shared interests or assumed as fundaments for the mutual defence principle within the EU no longer apply.

Hybrid conflicts are the synchronized use of multiple instruments of power tailored to specific vulnerabilities across a full spectrum of societal functions to achieve synergistic effects. In most cases, response mechanisms to hybrid threats are based on solid groundwork done on a national level, but the two organizations who share most of their members, whose critical structures and security are interconnected, cannot underestimate the risk posed to the mechanisms of collective security by a continuous low-intensity conflict. In order to be able to stem the dangers of the hybrid threat or limit the manoeuvring spaces of adversaries, which would give rise to an effective deterrent, it will be necessary for NATO and the Union to act in a coordinated manner on a legal level, as well. It is in the absolute interest of both to influence the relevant legal framework to guarantee the effectiveness and, above all, the credibility of Article 5 of the North Atlantic Treaty and Art. 42 of the Treaty on European Union. Only a very well-coordinated approach between the EU and NATO will guarantee the three main moments of any hybrid conflict: deterrence, attribution, resilience.

References

Cederberg A. Eronen P. Mustonen J. (2017). *Regional Cooperation to Support National Hybrid Defence Efforts. Helsinki: Hybrid COE*

European Commission (2018). *Joint Report to the European Parliament, the European Commission and the Council on the implementation of the Joint Framework on countering hybrid threats from July 2017 to June 2018. Retrieved from: https://cdn1-eeas.fpfis.tech.ec.europa.eu/cdn/farfuture/WlVziQJekWnYEhL-K2EEalHXejkn8YjlcDGjv4PCbRU/mtime:1528881150/sites/eeas/files/joint_report_on_the_implementation_of_the_joint_framework_on_countering_hybrid_threats_from_july_2017_to_june_2018.pdf*

Euroepan Council (2018). Third progress report on the implementation of the common set of proposals. Retrieved from: https://www.consilium.europa.eu/media/35578/third-report-ue-nato-layout-en.pdf

European Parliament (2017). *Briefing: Countering hybrid threats: EU-NATO cooperation. Retrieved from:http://www.europarl.europa.eu/RegData/etudes/BRIE/2017/599315/EPRS_BRI(2017)599315_EN.pdf*

European Union. (2016). *Visione condivisa, azione comune: un'Europa più forte. Retrieved from: https://europa.eu/globalstrategy/sites/globalstrategy/files/eugs_it_version.pdf*

European Union External Action (2018). A Europe that Protects: Countering Hybrid Threats. Retrieved from: ***https://eeas.europa.eu/topics/economic-relations-connectivity-innovation/46393/europe-protects-countering-hybrid-threats_en***

Gaiser L. (2017). *Resilient critical infrastructure and economic intelligence in the cyber domain. National security and the future. Vol. 18, no. 1/2.*

Gunneriusson H. Ottis R. (2013). Cyberspace from the Hybrid Threat Perspective. R.Kuusisto, E. Kurkinen (eds.), Proceedings of the 12th European Conference *on Information Warfare and Security. Jyväskylä : University of Jyväskylä.*

Halgestam N., Hagelstam A. (2018). *Cooperating to counter hybrid threats. Nato Review Magazine. 23/11/2018. Retrieved from:* **https://www.nato.int/docu/review/2018/also-in-2018/cooperating-to-counter-hybrid-threats/EN/index.htm**

Irmakkesen Ö. (2014). The Notion of Armed Attack under the UN Charter and the Notion of International Armed Conflict – Interrelated or Distinct? Paper presented at geneva Academy of International Humanitarian Law and Human Rights. Retrieved from: http://www.prix-henry-dunant.org/wp-content/uploads/2014_IRMAKKESEN_Paper.pdf

Kramer F. et alia (2015). *NATO's New Strategy: Stability Generation. Washington: Atlantic Council.*

MCDC, *https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/647776/dar_mcdc_hybrid_warfare.pdf*

NATO (2010). *Active engagement Modern Defence: Strategic Concept. Retrieved from: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/20120214_strategic-concept-2010-eng.pdf*

NATO (2016). *Joint Declaration. Retrieved from: https://www.nato.int/cps/en/natohq/official_texts_133163.htm?selectedLocale=en*

NATO(2018). *Response to hybrid threats. Retrieved from: https://www.nato.int/cps/en/natohq/topics_156338.htm*

NATO (2019). *Relations with the European Union. Retrieved from: https://www.nato.int/cps/en/natohq/topics_49217.htm*

Reichborn-Kjennerud E., Cullen P. (2016*). What is Hybrid Warfare?. Policy Brief, no. 1. Oslo: NUPI.*

Reichborn-Kjennerud E., Cullen P. (eds). (2017). *Understanding Hybrid Warfare. London: MCDC.*

Ventre D. (2016). *Information Warfare: second edition. London: Iste.*