

The Changing Security Landscape of Europe: Challenge of Hybrid Security Threats and War

DHAWLENDU

Ph.D. Research Scholar

Centre for European Studies, School of International Studies

Jawaharlal Nehru University, New Delhi (India)

ABSTRACT

The security landscape in Europe is experiencing a profound transformation, denoted by a change from traditional military threats to an exhibition of non-traditional security challenges. This paper delves into the evolving nature of threats, highlighting the notable elevation in hybrid security threats and warfare. It analyses the complex interplay between the growing use of cyberspace and the employment of hybrid warfare methods while examining a series of significant events that ultimately contributed to the study of hybrid warfare in international relations. Central to this discussion are the two primary security actors—the European Union (EU) and the North Atlantic Treaty Organization (NATO). Both play integral roles in safe guarding Europe, with the EU concentrating on political and economic integration and internal security, whereas, NATO delivers collective defence and military alacrity to prevent external threats. This paper provides a comprehensive outline of Europe's evolving security.

Keywords: Hybrid Security, Threats, Warfare, NATO, EU, Cooperation, Traditional and Non-traditional Security

INTRODUCTION

The global security landscape has been ever changing although it has never been so entangled for states as it is in the present globalised era of technological, informational, asymmetrical and extremely sensitive yet increasing contestations of power. The concept of hybrid threats is about the combination of conventional and unconventional, military and non-military, overt and covert activities that can be used in a multiple manner by state or non-state actors to accomplish specific goals while lingering below the verge of officially declared conflict alongside in times of war. They aim critical weaknesses and pursue to generate uncertainty; hampering swift and active decision-making. The variety of measures applied as part of a hybrid operation may be very extensive: from cyber-attacks on essential information systems through the disruption of critical services, such as energy supplies or financial services, to undermining public trust in

government institutions or manipulating social susceptibilities.

In recent years, the European security environment has also transformed and many of the current challenges to peace, security and prosperity originate from instability in its immediate and extended neighbourhood. These have a direct impact on the EU's internal and external security and call for the Union along with NATO to adapt and to mobilise its comprehensive toolbox with the objective of ensuring improved protection of its citizens, core values and infrastructure.

In his 2014 Political Guidelines, the Commission President Jean-Claude Juncker stressed the necessity “to work on a stronger Europe when it comes to security and defence” and to pool European and national instruments in a more effective approach than in the past.

In so far as countering hybrid threats relates to national security and defence, the primary accountability lies with Member States (MS), as most national exposures

are country specific. However, many member states face common threats that can be more successfully addressed at the EU level. Thus, it can play an imperative role in improving shared situational awareness, building Member States' resilience to hybrid threats, and most importantly in preventing, responding to and recovering from crisis.

Post the 2004 enlargement, it has been observed that conflict of values has the potential to enhance polarization and disunity within the EU, making them more vulnerable to external interferences. Intensifying contradictions between western values and authoritarian states erode the international norms and open democratic institutions make western societies easy targets of comprehensive hybrid attacks. The ongoing contestation of power at the international level with geoeconomics and geopolitics combined provide a fertile ground for hybrid security action.

Scope of the subject of Hybrid Threats and Warfare:

Hybrid threats are unleashed by covert and overt actions of traditional or non-traditional actors on vulnerabilities and decision-making abilities of the host state without crossing the threshold of detection, attribution, or retribution. In recent times, activities like influencing voter preferences in elections through social media, disinformation campaigns, cyber security threats, disruption in critical infrastructure services, trivializing social and political affairs, influencing public opinion or perception through social media, and inflicting direct attacks through proxies are undertaken in different degrees by different actors. It violates the credibility of democratic sovereign states by demoralizing and discrediting their structures, agents and processes by deploying technology as disruptor and thrive on post-truth partisan society's populism driven insecurities.

The international security setting is undoubtedly shifting and sprouting conflicts of hybrid characteristics connected with different problems. Security itself is a theoretical concept that has evolved over time. During the Cold War, security focused exclusively on traditional military aspects, however, by the 1980s, the concept of human security also grew to focus attention beyond the state. Since the end of Cold War, state and human security has come to be incorporated within the larger definition of security. Despite this, states and regions interpret the concept of security differently and hence there are different threat perceptions. The geopolitical events witnessed during the last decade in the periphery of

Europe have further exposed that the great power competition is growing in intensity and scope and significantly rivalry of values and narratives has been regenerated. Whether its Russia's annexation of Crimea in 2014, the ongoing Ukrainian war, aggravating Euroscepticism, miscommunication have posed new challenges to the Transatlantic partnership and the growing populism in Europe; all has made the EU re-examine the changing nature of threats.

Since the world affairs has become more complex and more connected in new ways, security analysis has been moving from resource-based power or the so-called hard power of the economy and the military towards relational power to influence others' principles, attitudes, preferences, views, outlooks, sentiments, or tendencies to act. In this type of situation, the awareness of hybridity, joining new and old apparatuses in an imaginative way turn out to be an attractive approach for those deficient of the competences or prospects to pursue their strategic interests otherwise. On the other hand, NATO as a dominant collective defence actor since 1949 tasked to protect the members has a strongly military based approach with a command-and-control system to deploy weapons. The NATO is unlike the EU, a defense organisation and has expanded its outreach after the end of Cold War and also reinvented itself. As threats have diversified and growing technology have impacted the security landscape, NATO also has to address the new hybrid threats.

The paper aims to examine the impact of the rise of hybrid security threats on the European security landscape. It analyses the response of two security actors in Europe- the EU and NATO towards the growth of hybrid threats and war. It will evaluate the EU's security strategy in context of evolving hybrid threats and assess its multi-dimensional approach. Similarly, it will examine the Strategic Concept of NATO to see how it has developed a new response to these new emerging threats and war. The annexation of Crimea in 2014 and the War in Ukraine in 2022 have been taken as reference point as this proved to be a watershed moment for the definitive shift in the security landscape of Europe when one observed the various dimensions of hybrid security threats come into play. There are not so comprehensive studies that have analysed the rise of hybrid security threats in the context of the annexation of Crimea, however, the war in Ukraine is a defining point in European security that shows the shift from hybrid threat

to hybrid war. The systematic analysis will examine the response of the EU and NATO since 9/11 to the 2022 war in Ukraine from the perspective of Hybrid security threats and war. Hybrid security Threats and war have transformed the European security landscape requiring the EU and NATO to develop countering strategies and work in partnership specially after the launch of the Ukraine war.

The Concept of Hybrid Security Threats and War:

Hybrid Security Threats and hybrid warfare/war are occasionally used alternately; thus, the notions can appear perplexing (Hybrid CoE, European Commission, 2021). In addition, the ideas of hybrid security have been examined through several diverse disciplinary lenses; prominent among them are history, political science, international relations, strategic studies, security studies, military studies etc. Although this multidisciplinary diagnostic assortment also hazes the depiction of what constitutes Hybrid Threats it is precisely for this reason that it should be studied as an umbrella concept.

Frank Hoffman, often viewed as the father of the idea of hybrid warfare concept, has said that his construction draws on numerous schools of strategic thinking, and manufactures intellectual synergies between the concepts of hybrid warfare and hybrid threats (Fridman, 2018). Hoffman's perception, which focused on non-state actors like Hezbollah and Al-Qaida, found that their strategic and operative military actions are directedly corresponding within the core battle space to accomplish synergistic properties (Fridman, 2018), including tactics used by transnational networks for organised crime and state actors. In recent times, specialists used the labels of "hybrid warfare", "new wars", fourth-generation warfare and asymmetric warfare, amongst others, to hypothesise changes in modern-day conflict. The concept refers to the impression that war had become "substantially distinct" from older patterns of conflict (Berdal, 2011). Indeed, the same Hybrid Threats concepts have evolved over time and encompassed every area governments deal with, not just purely in military terms.

Hybrid Threats concept mainly focuses on interferences and manoeuvres targeted against states and their institutions with various means. These concepts assert the question of systemic vulnerabilities of democratic systems as precise targets and undoubtedly argue for a comprehensive method with civil-military

collaboration from the very foundation. It is essential to understand that Hybrid Threats and War applies more to States having a democratic political system.

The concept has been adopted primarily by Russian and Chinese military thinking of using Hybrid Warfare tools against the Western countries. There is the language problem in understanding hybrid challenges while tracing the concept's roots in Western military and strategic discourse. It demonstrates that hybrid warfare and hybrid threats are different. Next, a conceptual distinction is made between hybrid warfare and hybrid threats to provide further clarity (Monaghan, 2019). The main obstacle to thinking clearly and uniformly about hybrid challenges is the problem of etymology. Terms coupling "hybrid" with the words "threats", "warfare", "activity", "operations" and "tactics" are repeatedly used interchangeably without definition. In contrast, notions such as "grey zone warfare," "competition short of war," and "modern political warfare" are too frequently commingled in the academic literature, policy publications and mainstream media (NATO, 2018, UK Government, 2015).

In 2005, the U.S. Lt Gen James Mattis—then Commanding General, Marine Corps Combat Development Command—and Frank Hoffman of the Center for Emerging Threats and Opportunities at Quantico reasoned that future adversary were likely to "mix and match" forms and modes of warfare to counterbalance conventional military battlefield authority (Mattis and Hoffman, 2005). Western military theorists were captivated by two big ideas that endangered the battleground's technological supremacy. The first was the threat posed by future adversaries merging types of warfare with non-military tools to overpower through compounding complications (Callard and Faber, 2003). The second was the problem of "non-trinitarian" adversaries who could not be conquered in "Clausewitzian" terms through a conventional military campaign concluding in a decisive battle (Creveld, 1991).

Meanwhile, actors elsewhere sought to make good on such fears by designing new ways of war that harnessed complexity and targeted Western vulnerabilities. Non-state actors such as al-Qaeda and Hezbollah undertook campaigns that put these principles into practice (Racz, 2018). In this form—as a description of how armed conflict was becoming more complex and challenging—the concept was incorporated into various approaches to international security strategy at the time,

for example, in the U.S., UK, and North Atlantic Treaty Organization (NATO) strategy documents (U.S. Quadrennial Defense Reviews, 2006, 2010; NATO, 2010; UK Ministry of Defence, 2010).

However, in mainstream discourse, hybrid warfare has taken on a much broader conception. It has been used to describe revisionist grand strategy that employs “a comprehensive toolset that ranges from cyber-attacks to propaganda and subversion, economic blackmail and sabotage, sponsorship of proxy forces and creeping military expansionism” (The Economist, 2010). It has also been commandeered by those looking for a snappy expression to pronounce the Kremlin’s art of strategy (Lucas, 2017, Jones, 2014, Barnes, 2016).

However, the term has since evolved through use, thriving in recent years throughout Euro-Atlantic security strategy documents in particular. For example, NATO has a “Counter Hybrid Threat Strategy” (NATO, 2018, European Commission, 2017), the European Union has developed a “playbook” for countering hybrid threats, and the European Countering Hybrid Threats Centre of Excellence was launched in Helsinki in 2017 (EEAS, 2017). In the UK 2015 Strategic Defense and Security Review, “hybrid threats” were classified as a “tier one” risk to national security and “hybrid attacks” on allies as a “tier two” risk (UK Government, 2015). While these interpretations differ somewhat in content, what they have in common is less to do with Hoffman’s hybrid warfare and more to do with Sun Tzu’s ancient wisdom that “to subdue the enemy without fighting is the acme of skill” (Monaghan, 2019).

Hybrid threats evolved as non- state actors and revisionist power sought to offset the strengths and target the vulnerabilities of the “status quo” powers. To achieve a counterweight of their own, hybrid aggressors target all three elements of Clausewitz’s “remarkable trinity” of the people, the government, and the military (Clausewitz, 1976) along with their complex dependencies between all three that reinforce the ability of any state to exercise power. Although this idea is not new, such a direct attack on society across the people, government, and military have frequently been reserved for the most intense hostilities in history.

The Russia annexation of Crimea in 2014 was accomplished through asset of “deniable” special militaries, local equipped proxies, economic instruments, deception, and manipulation of socio-political polarisation in Ukraine. Hybrid threats turn out to be a fundamental

security issue with Crimean annexation and now finally, leading to a full outbreak of hybrid warfare in the 2022 crisis of hostilities between Russia and Ukraine. The manoeuvring activities adopted by Russia completely transformed the security perception of European countries and sowed severe suspicion in ties between Moscow, the EU and the US. The Russian campaigns of invading Crimea and backing up the insurgents in eastern Ukraine, was just a teaser of hybrid warfare to the EU and NATO, and a signalling for what the future holds. The so- called Russian “peacekeeping force” that went into the separatist regions of Donbas, in Ukraine was led by an upsurge of the largest attacks of its kind with cyber and information tools involving banks, ministries of defence, foreign, cultural and even, the army.

The modus operandi appears to be evolved from the persistent hybrid warfare strategies adopted by powerful states like Russia against their different opponents in recent years. There is straight link between the 2014 Russian annexation of Crimea and with the current series of events unfolding in and around Ukraine of 2022, it exemplifies Russia trying to perfect its hybrid warfare playbook through means of new practices and learning from the West’s responses. The “little green men” in annexation of Crimea and the “little blue men” in capturing of the South China Sea was the manifestation of the clue that international struggle might be destined for more hybrid warfare and hybrid threats and thus, has influenced security and defence deliberations in establishments of European Union, NATO and beyond.

The Response of EU in the face Hybrid Security Threats and War:

In 1992, with the Masstricht Treaty, the EU introduced innovative and comprehensive approach towards Common Foreign and Security Policy, internalisation of the Common Security and Defence Policy, and interconnectedness of security ties. The evolution of the EU as a security actor is still an ongoing process. Important documents like the ESS 2003 and the EUGS 2016 reveal the maturing of the actor. Both documents give an insight into the security threats identified by the Union and the strategy of addressing the growing and varying challenges.

The European Union comprehends hybrid operations as ‘multidimensional, combining coercive and subversive measures, using conventional and unconventional tools and diplomatic, military, economic, and technological

tactics to undermine the opponent. These operations are designed to be hard to attribute or detect and can be utilised by the state and non-state actors' (European Commission/High Representative of the Union for Foreign Affairs and Security Policy, 2018).

At the operational level, the EU has steered the largest ever tabletop exercise on Hybrid Threats called Parallel and Coordinated Exercise (PACE 18) in partnership with NATO. These exertions leave no doubt on the standing of the EU on Hybrid Threats. The need for a solid conceptual basis that removes hindrances for relevant stakeholders to expand their understanding of hybrid threats has been addressed by the Joint Research Centre of the European Commission and the European Centre of Excellence for Countering Hybrid Threats in Helsinki. Different forces are joined across the EU to deal with challenges for designing and implementing effective measures to deal with this very complex phenomenon.

The EU Security Union Strategy for the period 2020 to 2025 also emphasized 'Security' as a cross-cutting subject affecting every scope of life and touches a multitude of policy extents. With the new Strategy, a real security ecosystem promised to be constructed overcoming the misleading dichotomy between online and offline, amid digital and physical and among internal and external security apprehensions. From defending critical infrastructure to hostile cyber crime and answering hybrid threats, all becomes pertinent for security in this strategy as an umbrella framework based on common EU values.

The strategy asserts on countering hybrid threats that are aimed at destroying the social cohesion and weaken faith in institutions, along with strengthening EU resilience to address these new challenges. A major dimension includes an EU tactic for dealing with hybrid threats, from primary discovery, investigation, responsiveness, building flexibility and deterrence to emergency comeback and consequence administration and in large, mainstreaming hybrid reflections into wider policy-paradigm in close cooperation with strategic partners, particularly NATO and G7.

In aspirational terms, the EU is slowly reinterpreting a role in leveraging its broad non-military skill set to complement the EU Member State military and intelligence and NATO counter-hybrid efforts. The EEAS paper from 2015 with a section entitled 'defining hybrid threats' began by noting that 'hybrid warfare can be more easily characterised than defined'. The EEAS has

discussed the possibility of this EU-NATO synergy at the strategic level, explaining that both organisations bring different competencies to bear. There is a rare chance to collaborate on building complementary and mutually supportive strategies while retaining the autonomy of actions in both organisations. Thus, even though the EU continues to emphasise that member states have 'the primary responsibility' for countering hybrid threats as a matter of national defence – not least because 'most national vulnerabilities are country-specific' – the EU sees an important and even necessary role for itself in countering hybrid threats.

The Commission President Jean-Claude Juncker, in his 2014 Political Guidelines, emphasised the necessity "to work on a stronger Europe when it comes to security and defence" and to pool European and national tools in a more practical approach than in the past (European Commission, 2016). In May 2015, the Foreign Affairs Council urged the High Representative to cooperate with the Commission, the Member States and the European Defence Agency and submit a Joint Framework with actionable recommendations to aid in neutralising hybrid threats, also underscoring the necessity to collaborate and bring together relevant partner organisations, comprising especially NATO, along with member countries, as suitable. In June 2015, the European Council further strengthened this mandate. Responding to these appeals, the Joint Framework aims to enable a holistic approach that will empower the EU to harmonise with the Member States to offset threats of a hybrid nature by producing synergies between different mechanisms and nurturing close cooperation between all pertinent actors (European Commission, 2016).

Since countering hybrid threats pertains to national security and defence, the primary accountability lies with the Member States. Then again, many Member States face similar threats that can be more successfully addressed at the EU level. The EU can be utilised as a platform to enhance national endeavours and, through its regulatory capacity, ascertain standard benchmarks that can help advance the level of protection and resilience throughout the Union. Hence, the EU can play an important role in cultivating shared situational awareness, developing Member States' resistance to hybrid threats, and thwarting, responding to, and recuperating from a crisis.

NATO's New Strategic Concept and Strategy for Hybrid Security Threats and War

NATO describes hybrid threats as 'those posed by adversaries, with the ability to simultaneously employ conventional and non-conventional means adaptively in pursuit of their objectives' (Miklaucic, 2011).

The Strategic Concept is a key document for the Alliance and the latest was presented in June 2022. It not only reaffirms NATO's values and purpose, and provides a collective assessment of the security environment and also drives its strategic adaptation and guides its future political and military development. The NATO 2030 initiative along ensures the Alliance remains prepared at present to face tomorrow's trials signaling a major focus of coming strategies and capabilities dedicated to hybrid challenges. The strategic concept asserts that prognosis of war is more dangerous in this competitive security insecure world.

The North Atlantic Treaty Organization's Strategic Concept is highly politically significant and next to the Washington Treaty, which is the basis of this security cooperation. Reviewed and updated regularly every 10 years, the Concept take account of variations to the global security situation since the cold war to make the Alliance ready for the future. The last Strategic Concept at the 2010 NATO Summit in Lisbon, Portugal gave the way for the Alliance to revolutionize its capability to carry out its essential undertaking of collective defence, cooperative security and sincere crisis management with promotion of global stability. It urged member states to capitalize key competences to meet emergent coercions with respect to hybrid domain along with the controversial question of NATO membership for European democracies. For an inclusive agenda, the Strategic Compass has brought the EU hybrid toolbox to bring together appropriate instruments like the cyber diplomacy toolbox and the Foreign Information Manipulation and Interference toolbox. It aims to expand the efficiency and consistency of diverse actions, agents and therefore fetch additional worth to the EU's capacity to respond.

Resilience, Preparedness and Cooperation between EU and NATO for Dealing with Hybrid Threats and War:

Resilience, Preparedness and Cooperation in the EU and NATO in backdrop of the outbreak of Hybrid War in Ukraine will be the ultimate focus on the concluding theme of this study. The first and crucial stage to achieve

better security against hybrid threats is to attain proper situational awareness. This is why intelligence and information sharing has become so vital. It is pre-eminent to augment the resilience of societies and critical infrastructure in order to avert and respond to hybrid threats efficiently. Considering the character of hybrid threats, it is crucial to work across geographical borders and agency boundaries.

A glance through the concept of hybrid threat to the challenges being posed by it not only from the security point of view but also to the existence of democracy and rule of law, now brings us to the major players involved in countering the problem: the European Union (EU) and the North Atlantic Treaty Organization (NATO).

NATO was the most successful collective security arrangement among states in the 20th century. Having deterred and outlasted its primary adversary, the Soviet Union, NATO now faces the challenge of redefining its roles and purposes in the 21st century. The Strategic Concept adopted by heads of state and government in Lisbon in November 2010 reconfirms the NATO commitment to "deter and defend against any threat of aggression, and against emerging security challenges where they threaten the fundamental security of individual Allies or the Alliance as a whole." It offers itself as the strategic map for NATO in the 21st century and touches on extremism, terrorism, and such transnational illegal activities as trafficking in arms, narcotics, and people, as well as cyber-attacks and other technological and environmental threats.

The Russian annexation of Crimea and the use of hybrid warfare methods has made the NATO re-look its strategy on fighting the war which was all but inevitable. It developed a strategy for its role in countering hybrid warfare to help address these threats. Since 2016, the Alliance has publicly stated that hybrid actions against one or more Allies could lead to a decision to invoke Article 5 of the North Atlantic Treaty. In July 2018, NATO leaders agreed to set up counter-hybrid support teams, which provide tailored targeted assistance to Allies upon their request, in preparing against and responding to hybrid activities. In July 2022, NATO Leaders endorsed comprehensive preventive and response options to counter hybrid threats. These can be tailored to address specific situations.

However, there is no consensus among the NATO member states on 'how and when' the Alliance should act in the hybrid domain. Some member states regard

NATO action in this area as potentially provocative and escalatory. In their view, NATO should be called upon for high-end military tasks only, and not if the threats remain under the threshold of Article 5.

The EU's wider set of responsibilities and tools makes the organisation better suited to play a bigger role in the hybrid domain in comparison to NATO. The EU began by getting a clear definition of the term 'hybrid warfare.' In the EU's 2016 Joint Communication the concept of a hybrid threat is defined as a mixture of coercive and subversive activity, using conventional and unconventional methods (*i.e.* diplomatic, military, economic and technological), coordinated by state or non-state actors to achieve specific objectives while remaining below the threshold of formally declared warfare (European Commission, 2016b).

The second important step in the direction of countering hybrid threats was to agree on strategic practical steps to be implemented by the EU and its member states. In April 2016, the European Commission and the High Representative of the EU for Foreign Affairs and Security Policy approved the Communication Joint Framework on Countering Hybrid Threats: A European Union Response, which has become a fundamental document in terms of structuring EU efforts in this area (European Commission, 2016b). A critical step in the right direction was the decision to establish the Hybrid CoE (Centre of Excellence) in April 2017. Established by 9 like-minded EU and NATO states, the centre's membership had grown to include 27 participating states by the end of 2019, with more candidates due to join.

In March 2022, the EU adopted The Strategic Compass which launched the development of an EU Hybrid Toolbox. It can be described as a way of working within the EU to enhance coherence between the multitude of instruments that the EU and its member states have to offer in countering hybrid threats. Its aim is to ensure that in case of a hybrid attack, the EU can offer a well-informed, targeted, and comprehensive response. The initiative to use the Toolbox lies with the member states, but it can also be used to assist EU partner countries.

Conclusion:

In the European context, the emergence of hybrid challenges not only had a political impact on how the EU and member states collectively address it, but it has also

had consequences on its institutional architecture, leading to essential adaptations within the EU itself. These institutional developments are meaningful from a European political and operational point of view and for potential cooperation with other partners, namely with NATO.

From a political perspective, it formally signals how the EU perceives and assesses the importance of hybrid threats and their disruptive potential. From an operational perspective, it underlines the collective intent and capacity of the EU to protect and rapidly respond to a new scale of security threats.

However, with the ambiguity and multi-dimensionality associated with the hybrid threats, there is no one clear way of approaching it. Moreover, in the present time, with technological developments happening at an ever-growing pace, there is a restriction on the capability to identify malicious practices post factum. The evolution of the available tools increases the reach and effectiveness of hybrid warfare in the pursuit of strategic objectives such as undermining public trust in institutions, gaining geopolitical influence and hampering institutional decision-making capabilities (Hybrid CoE, 2019, 10). Furthermore, the effectiveness of such tactics hinges on their ability to exploit the core principles, laws and values that govern democratic societies. The open pluralism of European democracies has and continues to be exploited to exacerbate existing ethnic, religious, political, or economic fault-lines, thereby undermining societal cohesion. This new dimension of insecurity has also strengthened European cooperation with NATO, in both the hybrid and the cyber contexts. Considering the challenges they pose to democratic systems; it is not surprising that tackling hybrid threats has been defined as a priority for EU- NATO member states.

REFERENCES

- Aaronson, M., Sverre, D., Yves De K., Mary, B.L. and Michael, M. (2011). NATO: Countering the Hybrid Threat. *PRISM*, 2 (4): 111–24.
- Bajarunas, E., (2020). Addressing Hybrid Threats: Priorities for the EU in 2020 and Beyond. *European View*, 19 (1) : 62–70.
- Bajarunas, E. and Kersanskas, V. (2018). Hybrid threats: Analysis of their content, challenges posed and measures to overcome. *Lithuanian Annual Strategic Review*, 16 (1):123-170, [Online: web] Accessed 14 February 2020 URL: <https://doi.org/10.2478/lasr-2018-0006>.

- Banim, G. and Pejsova, Eva (eds) (2017). Prevention better than cure: the EU's quiet diplomacy in Asia. *EU Institute for Security Studies*, 33.
- Barnes, J.E. (2016). NATO Works to Adapt to More Ambiguous Warfare Techniques. *Wall Street Journal*, 8.
- Berdal, Mats (2011). The 'New Wars' Thesis Revisited" in Hew Strachan, Sibylle Scheipers (eds) *The Changing Character of War*, Oxford: Oxford University Press.Brussels.
- Caliskan, M. (2019). Hybrid warfare through the lens of strategic theory. *Defense & Security Analysis*, 35(1) : 40-58.
- Callard, J. and Faber, P. (2002). An Emerging Synthesis for a New Way of War. *Georgetown J. Internat. Affairs*, 3 (1):61-68.
- Clausewitz, Carl (1976). *On War*, Translated by Michael Howard and Peter Paret (eds), Princeton: Princeton University Press, reprinted 1989.
- Costa, R. (2021). Hybrid Threats in the Context of European Security: Report of the international conference organized at the National Defence Institute (IDN) on 18 May 2021 under the framework of the Portuguese Presidency of the Council of the European Union. *Instituto da Defesa Nacional*, E-Briefing Papers, [Online: web] Accessed 16 June 2021, URL: <https://www.idn.gov.pt/pt/publicacoes/ebriefing/Documents/E-Briefing%20Papers/E-Briefing%20Papers%203.pdf>
- Council of the EU (2015). Food for Thought Paper "Countering Hybrid Threats", *EEAS*, 8887/15, [Online: web] Accessed 20 April 2020 URL: <https://www.statewatch.org/media/documents/news/2015/may/eeas-csdp-hybrid-threats-8887-15.pdf>
- Council of the EU (2016). Joint Staff Working Document EU operational protocol for countering hybrid threats 'EU Playbook. *Council of the EU*, SWD(2016) 227 final, Brussels.
- Council of the EU (2017). *Eastern Partnership Summit – Joint declaration*, Press Release, 695/17, 24 November, [Online: web] Accessed 14 February 2020 URL: <https://data.consilium.europa.eu/doc/document/ST-14821-2017-INIT/en/pdf>
- Cullen, P., Juola, C., Karagiannis, G., Kivisoo, K., Normark, M., Rácz, A., Schmid, J. and Schroefl, J. (2021). *The landscape of Hybrid Threats: A Conceptual Model* (Public Version), Giannopoulos, G., Smith, H. and Theodoridou, M. (eds.), EUR 30585 EN, Luxembourg: Publications Office of the European Union.
- Cullen, Patrick J. and Erik Reichborn-Kjennerud (2017). MCDC Countering Hybrid Warfare Project: Understanding Hybrid Warfare. *Multinational Capability Development Campaign/NATO Allied Command Transformation*.
- Damien Van Puyvelde (2015). Hybrid War: Does it Even Exist?, *NATO Review*, 2015, <https://www.nato.int/DOCU/review/2015/Alsoin-2015/hybrid-modern-future-warfare-russia-ukraine/EN/index.htm>.
- Dengg, A. and Schurian, Michael N. (2016). On the Concept of Hybrid Threats, in Anton Dengg and Michael N Schurian (eds) *Networked Insecurity – Hybrid Threats in the 21st Century*, Vienna: National Defence Academy, Vienna.
- Deshpande, V. (2018). Hybrid warfare: the changing character of conflict. Pentagon Press and Institute for Defence Studies and Analyses, New Delhi.
- Drent, M., Hendriks, R. and Zandee, D. (2015). *New threats, new EU and NATO Responses*. The Hague, Netherlands: Clingendael Institute.
- EEAS (2017). EU and NATO inaugurate European Centre of Excellence for Countering Hybrid Threats, *EEAS*, 731, [Online: web] Accessed 17 March 2020 URL: https://eeas.europa.eu/delegations/gabon/33119/eu-and-nato-inaugurate-european-centre-excellence-countering-hybrid-threats_az
- Élie Tenenbaum, (2015). Hybrid Warfare in the Strategic Spectrum: An Historical Assessment in Guillaume Lasconjarias and Jeffrey A. Larsen (eds) *NATO's Response to Hybrid Threats*, Rome: NATO Defence College.
- European Commission (2016). Shared vision, common action: A stronger Europe—a global strategy for the European union's foreign and security Policy, *EU Commission*, Brussels.
- European Commission (2016a). Joint Framework for Countering Hybrid Threats, *European Commission*, Brussels.
- European Commission (2016b). Stronger and Smarter Information Systems for Borders and Security, *Communication From The Commission To The European Parliament and The Council*, COM(2016) 205 final, Brussels, [Online: web] Accessed 23 November 2020 URL: https://ec.europa.eu/home-affairs/system/files/2020-09/communication_on_stronger_and_smart_borders_20160406_en.pdf
- European Commission (2017). Security and Defense: Significant Progress to Enhance Europe's Resilience against Hybrid Threats—More Work Ahead, *European Commission Press Release*, 19 July, Brussels, URL: https://ec.europa.eu/commission/presscorner/detail/en/IP_17_2064.
- European Commission (2017a). Joint Report to the European

Parliament and the Council on the implementation of the Joint Framework on countering hybrid threats - a European Union response. *European Commission*, JOIN/2017/030 final, Brussels.

European Commission (2018). Joint Communication to the European Parliament, the European Council and the Council Increasing resilience and bolstering capabilities to address hybrid threats, *European Commission*, JOIN/2018/16 final,

European Commission (2018a). Joint Report to the European Parliament, the European Council and the Council on the implementation of the Joint Framework on countering hybrid threats from July 2017 to June 2018, *European Commission*, JOIN (2018) 14 final, Brussels.

European Commission (2020). Communication From The Commission To The European Parliament, The European Council, The Council, The European Economic And Social Committee And The Committee of the Regions on the EU Security Union Strategy, *European Commission*, COM/2020/605 final, Brussels.

European Commission (2020a). Joint Staff Working Document 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, *European Commission*, SWD (2020)153, Brussels.

European Commission and High Representative of The Union for Foreign Affairs and Security Policy (2020). Joint Staff Working Document Mapping of measures related to enhancing resilience and countering hybrid threats, *European Commission*, SWD (2020) 152 final, Brussels.

European Commission and High Representative of The Union for Foreign Affairs and Security Policy (2021). Joint Staff Working Document: Fifth Progress 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, Brussels, SWD (2021) 729.

European Commission, Joint Communication to The European Parliament, The European Council and The Council (2018). https://ec.europa.eu/info/sites/default/files/joint-communication-eu-us-agenda_en.pdf

European Commission, Joint Communication to The European Parliament, The European Council and The Council, press release, (2017). http://europa.eu/rapid/press-release_IP-17-2064_en.htm

European Commission, Joint Communication to The European Parliament, The European Council and The Council (2016a). Delivering on the European Agenda on Security

to fight against terrorism and pave the way towards an effective and genuine Security Union. Communication, COM (2016) 230 final, 20 April.

European Commission, Joint Communication to The European Parliament, The European Council and The Council (2017). A strategic approach to resilience in the EU's external action. Communication, JOIN (2017) 21 final, 7 June. https://ec.europa.eu/knowledge4policy/publication/2017-joint-communication-strategic-approach-resilience-eus-external-action_en. Accessed 14 February 2020.

European Commission (2018a). Action plan against disinformation. Communication, JOIN (2018) 36 final, 5 December. https://ec.europa.eu/commission/sites/beta-political/files/eucommunication-disinformation-euco-05122018_en.pdf. Accessed 14 February 2020.

European Commission (2018b). Increasing resilience and bolstering capabilities to address hybrid threats. Communication, JOIN (2018) 16 final, 13 July. https://eeas.europa.eu/sites/eeas/files/joint_communication_increasing_resilience_and_bolstering_capabilities_to_address_hybrid_threats.pdf. Accessed 14 February 2020.

European Commission/High Representative of the Union for Foreign Affairs and Security Policy (2018), Joint Communication on Increasing Resilience and Bolstering Capabilities to Address Hybrid Threats, JOIN 16 final, Brussels, 13 June.

European Council (2016). Joint declaration by the President of the European Council, Donald Tusk, the President of the European Commission, Jean-Claude Juncker, and the Secretary General of NATO, Jens Stoltenberg, *Press Release of European Council*, 8 July, [Online: web] Accessed 14 February 2020 URL: <https://www.consilium.europa.eu/en/press/press-releases/2016/07/08/eu-nato-joint-declaration/>.

European Council (2018). European Council meeting (22 March 2018) – Conclusions, EUCO 1/18, 23 March, Brussels, [Online: web] Accessed 14 February 2020 URL: <https://www.consilium.europa.eu/media/33457/22-euco-final-conclusions-en.pdf>.

European Council (2019). 'A new strategic agenda, 2019–2024'. *European Council Press Release*, 20 June. URL: <https://www.consilium.europa.eu/en/press/press-releases/2019/06/20/a-new-strategicagenda-2019-2024/>.

European Council (2019a). 'Countering hybrid threats: Council calls for enhanced common action'. *Council of the EU Press Release*, 10 December. URL: <https://www.consilium.europa.eu/en/press/press-releases/2019/12/10/countering-hybrid-threats-council-calls-for-enhanced-common-action/>.

- European Defense Agency (2015). "Hybrid Warfare", May, URL: <https://www.eda.europa.eu/what-we-do/activities/activities-search/hybrid-warfare>.
- Fernández, Luciana M. (2009). Laws in the Era of Hybrid Threats. *Hybrid CoE Strategic Analysis*.
- Fiott, D. and Parkes, R. (2019). Protecting Europe: The EU's response to hybrid threats. *European Union Institute for Security Studies*, Chaillot Paper, 151.
- Freedman, L. (2015). *Strategy: A history*, Oxford: Oxford University Press.
- Fridman, O. (2018). *Russian "Hybrid Warfare": Resurgence and Politicization*, Oxford: Oxford University Press.
- Friends of Europe (2018). "Hybrid and Transnational Threats. *Discussion Paper*, December.
- Galeotti, M. (2018). (Mis) Understanding Russia's Two 'Hybrid Wars', *Êðèòèà è ðòìàèùì*, (49), 17-27.
- Gressel, G. (2019). Protecting Europe Against Hybrid Threats. *Policy Brief European Council on Foreign Relations*, 25 June.
- Hoffman, F.G. (2009). Hybrid threats: Reconceptualizing the evolving character of modern conflict. *Strategic Forum*, Institute for National Strategic Studies, National Defense University, 240: 1-8.
- Hoffman, Frank G. (2007). *Conflict in the 21st Century: The Rise of Hybrid Wars*, Arlington: Potomac Institute for Policy Studies.
- Hoffman, Frank G. (2010). 'Hybrid Threats': Neither Omnipotent nor Unbeatable. *Orbis*, 54 (3): 441-55. <https://doi.org/10.1016/J.ORBIS.2010.04.009>.
- Howard, M. (2000). *The invention of peace: Reflections on war and international order*, New Haven: Yale University Press.
- Hybrid, CoE (2018). "Hybrid Threats", *The European Centre of Excellence for Countering Hybrid Threats*, 14 January 2018, [Online: web] Accessed 14 February 2020 URL: <https://www.hybridcoe.fi/hybrid-threats/>.
- Joint Communication to the European Parliament and the Council, Joint Framework on countering hybrid threats: a European Union response (2016), European Commission JOIN (2016) 18 final.
- Jones, S. (2014). Ukraine: Russia's new art of war, *Financial Times*, 28 August.
- Jordan, D., James D. Kiras David J. Lonsdale, Ian Speller Christopher Tuck and C. Dale Walton Frontmatter (2008) *Understanding Modern Warfare*. Cambridge: Cambridge University Press
- Kofman, M. and Rojansky, M. (2015). A Closer look at Russia's "Hybrid War". *Kennan Cable*
- Lasconjarias, G. and Larsen, J.A. (2015). Introduction: A New Way of Warfare in Guillaume Lasconjarias and Jeffrey A. Larsen (eds.) *NATO's Response to Hybrid Threats*, Rome: NATO Defence College.
- Lind, W.S., Nightengale, K., Schmitt, J.F., Sutton, J.W. and Wilson, G.I. (2001). The changing face of war: Into the fourth generation. *Marine Corps Gazette*, 85(11): 65-68.
- Lucas, E. (2017). We Must Wake Up to Russia's Shifting Threats. *The Times*, 27 October 2017.
- Lyne, R. et al. (2015), *The Russian Challenge*, London: Chatham House, the Royal Institute of International Affairs.
- Mälksoo, M. (2018), "Countering hybrid warfare as ontological security management: the emerging practices of the EU and NATO", *European Security*, 27(3): 374-392, DOI: 10.1080/09662839.2018.1497984
- Mattis, James N. and Hoffman, F.G. (2005). Future Warfare: The Rise of Hybrid Wars. Proceedings-United States Naval Institute, 131(11): 18.
- Miklaucic, M. (2011). "NATO Countering the Hybrid Threat", *NATO Allied Command Transformation*, 23 September, [Online: web] Accessed 14 February 2020 URL: <https://www.act.nato.int/nato-countering-the-hybrid-threat>.
- Mitrovic, M. (2017). Hybrid Security Threats and Contemporary Approach to National Security, Thematic Conference Proceedings of International Significance, International Conference "Archibald Reiss Days. *Academy of Criminal and Police Studies*, Belgrade, 1: 337-345, [Online: web] Accessed 14 February 2020 URL: <https://ssrn.com/abstract=3070803>
- Mölling, C. (2015). From Hybrid Threats to Hybrid Security Policy. *Ethics & Armed Forces*, 2015/2.
- Monaghan, A. (2015). The 'war' in Russia's 'Hybrid Warfare'. *Parameters*, 45(4).
- Monaghan, S. (2019). Countering Hybrid Warfare: So, What for the Future Joint Force? *PRISM*, 8 (2): 82-99, [Online: web] Accessed 14 February 2020 URL: https://ndupress.ndu.edu/Portals/68/Documents/prism/prism_8-2/PRISM_8-2_Monaghan.pdf
- Najžer, B. (2020). *The Hybrid Age: International Security in the Era of Hybrid Warfare*, UK: Bloomsbury Academic.
- NATO (2010). "Bi-SC Input to a New NATO Capstone Concept for the Military Contribution to Countering Hybrid Threats", *NATO Military Committee*, Brussels, [Online: web] Accessed 14 February 2020 URL: www.act.nato.int/images/stories/events/2010/20100826_bi-sc_cht.pdf

- NATO (2018). "NATO's Response to Hybrid Threats", *NATO, Topics*, [Online: web] Accessed 14 February 2020 URL: www.nato.int/cps/en/natohq/topics_156338.htm
- NATO (2018a). Brussels Summit Declaration, *Press Release of NATO*, (2018) 074, 11 July, [Online: web] Accessed 14 February 2020 URL: https://www.nat11Jul.2018o.int/cps/en/natohq/official_texts_156624.htm
- NATO (2022). Strategic Concept 2022, Adopted by Heads of State and Government at the NATO Summit in Madrid 29 June 2022, <https://www.nato.int/strategic-concept/>
- Pindják, Peter (2014). "Deterring Hybrid Warfare: A Chance for NATO and the EU to Work Together?", *NATO Review*, 18 November 2014.
- Racz, A. (2018). The Role of Military Power in Russia's New Generation Warfare Arsenal in Ukraine and Beyond, [Online: web] Accessed 14 February 2020 URL: https://www.academia.edu/37619239/The_Role_of_Military_Power_in_%20Russias_New_Generation_Warfare_Arsenal_in_%20Ukraine_and_Beyond
- Raitasalo, J. (2017). Getting a Grip on the So-Called "Hybrid Warfare", *ASPJ Africa & Francophonie*, 3rd Quarter: 20-39.
- Renz, B. and Smith, H. (2016). Russia and Hybrid Warfare - Going beyond the Label. *Aleksanteri Papers*, 1/2016.
- Smith, H. (2017). In the Era of Hybrid Threats: Power of the Powerful or Power of the 'Weak'?" *Hybrid CoE Strategic Analysis*.
- Smith, H. (2019). "Countering Hybrid Threats", in Gustav Lindstrom and Thierry Tardy (eds), *The EU AND NATO: The essential partners*, Paris: EUISS.
- Tenenbaum, É. (2015). Hybrid Warfare in the Strategic Spectrum: An Historical Assessment in Guillaume Lasconjarias and Jeffrey Larsen (eds.) *NATO's Response to Hybrid Threats*, Rome: NATO Defence College, 30 December, 95-112.
- The Economist (2018). "Shades of Grey: Neither War nor Peace", *The Economist*, 25 January 2018, [Online: web] Accessed 14 February 2020 URL: <https://www.economist.com/special-report/2018/01/25/neither-war-nor-peace>
- Thiele, Ralph D. (2016). Building Resilience Readiness against Hybrid Threats – A Cooperative European Union / NATO Perspective, *ISPSW Strategy Series: Focus on Defense and International Security*, 449, September, [Online: web] Accessed 19 October 2020 URL: https://www.ispsw.com/wp-content/uploads/2016/09/449_Thiele_Malaysia_Sep2016.pdf
- Tzu, S. (2009). *The Art of War*. UK: Amazon.
- U.S. Quadrennial Defense Reviews (2006, 2010). Department of Defense, U.S.
- UK Government (2015). National Security Strategy and Strategic Defence and Security Review 2015 A Secure and Prosperous United Kingdom, *Policy Paper of UK Government*, November, [Online: web] Accessed 19 October 2020 URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/478936/52309_Cm_9161_NSS_SD_Review_PRINT_only.pdf
- Uzieblo, Jan J. (2017). 'United in Ambiguity? EU and NATO Approaches to Hybrid Warfare and Hybrid Threats', *EU Diplomacy Paper*, College of Europe, Brugge.
- Van Creveld, M. (1991). *The Transformation of War*, New York: Simon and Schuster.
- van der Putten, Frans-Paulet al. (eds) (2018). *Hybrid Conflict: The Roles of Russia, North Korea and China*. The Netherlands Institute of International Relations 'Clingendael'.
- Weissmann, M., Nilsson, N., Palmertz, B. and Thunholm, P. (eds) (2021). *Hybrid Warfare: Security and Asymmetric Conflict in International Relations*, London: Bloomsbury Publishing, I.B. TAURIS.
- Wigell, M. et al. (2021). Best Practices in the whole-of-society approach in countering hybrid threats, *Study, Policy Department for External Relations, Directorate General for External Policies of the Union*, PE 653.632, May.
- Wigell, Mikael (2019). Hybrid Interference as a Wedge Strategy: A Theory of External Interference in Liberal Democracy, *Internat. Affairs*, **95** (2): 255–75. <https://doi.org/10.1093/ia/iiz018>.
- Wilkie, R. (2009). Hybrid Warfare: Something Old, Not Something New. *Air & Space Power J.*, **23** (4): 13-18.
- Williamson, M. and Mansoor, Peter R. (eds) (2012). *Hybrid Warfare: Fighting Complex Opponents from Ancient World to the Present*, Cambridge: Cambridge University Press.
- Zwolski, K. (2018). *European Security in Integration Theory: Contested Boundaries*, Southampton, UK: Palgrave Macmillan.
