XLV POLISH YEARBOOK OF INTERNATIONAL LAW
2025 DOI 10.24425/PYIL.2026.3105
PL ISSN 0554-498X
e-ISSN 2957-1510

*Agata Kleczkowska**

NEITHER PEACE NOR WAR: INTERNATIONAL LAW IN TIMES OF NONCONVENTIONAL THREATS

Abstract: *The article aims to initiate a discussion on whether and, if so, what kind of changes are needed for international law to remain an effective instrument of response for the international community in the face of hybrid threats. Thus, it is also a question of how international law should be shaped in future to safeguard the international rule of law and help democratic societies remain resilient against attacks from totalitarian regimes. To this end, the article is divided into two parts. The first suggests that while international law remains applicable, its existing structures and doctrines are strained by the nature of the security challenges Europe currently faces, necessitating legal adjustments. The second proposes three changes that scholars should consider for further discussion and that could render international law more adequate in times when nonconventional threats are becoming the primary means of conflict between States.*

Keywords: countermeasures, fundamental standards of humanity, hybrid threats, principle of non-intervention, Russia

INTRODUCTION

In September 2025, German Chancellor Friedrich Merz said that Europe "is not at war [...] but no longer at peace" with Russia.[1] A month later, Polish Minister of

* PhD, Assistant Professor; Institute of Law Studies of the Polish Academy of Sciences (Poland); e-mail: agata.kleczkowska@inp.pan.pl; ORCID: 0000-0003-4621-6336. The research for this article was funded in whole by the National Science Centre, Poland within the research project "Retorsions in public international law" (2020/39/B/HS5/03383).

Defence Władysław Kosiniak-Kamysz asserted that "[w]e need to change the way of thinking that we live neither in a time of war nor in a time of peace."[2] A similar statement was also made by NATO Secretary General Mark Rutte by the end of 2024, although he appeared to refer to a broader group of potential adversaries, including not only Russia but also China, North Korea and Iran.[3] While such proclamations may be regarded as a neat figure of speech, it is increasingly difficult to ignore that they accurately describe the complex reality in which Europeans currently live. While this difficulty is visible on many levels – political, economic, diplomatic and military – it also affects the ability to assess the security challenges that Europe currently faces from the perspective of international law.

This short article aims to initiate a discussion on whether and, if so, what kind of changes are needed for international law to remain an effective instrument of response for the international community in the face of different non-conventional threats, often collectively called hybrid threats,[4] including disinformation,[5] cyber-attacks,[6] physical operations against infrastructure, financing cultural groups and think tanks, election interference and many more. Thus, it is also a question of how

---

[1] *Europe 'no longer at peace' with Russia, says Germany's Merz*, Reuters, 29 September 2025, available at: https://www.reuters.com/world/europe-no-longer-peace-with-russia-says-germanys-merz-2025-09-29/ (accessed 31 March 2026).

[2] P. Wyżga, K. Bogdańska, *Władysław Kosiniak-Kamysz: Polska musi być gotowa na najgorsze, ale zbroi się na pokój* [Władysław Kosiniak-Kamysz: Poland must be ready for the worst, but it is arming itself for peace], WP, 25 October 2025, available at: https://wiadomosci.wp.pl/wladyslaw-kosiniak-kamysz-polska-musi-byc-gotowa-na-najgorsze-ale-zbroi-sie-na-pokoj-7213950444972992a (accessed 31 March 2026).

[3] *Speech by NATO Secretary General Mark Rutte at the Concert Noble, Brussels*, 12 December 2024, available at: https://www.nato.int/en/news-and-events/events/transcripts/2024/12/12/to-prevent-war-na-to-must-spend-more (accessed 31 March 2026).

[4] Following the definition of the European Centre of Excellence for Countering Hybrid Threats, "hybrid threats" are understood herein as harmful activities planned and carried out with malign intent to undermine a target, such as a State or an institution, through a variety of means, often combined (*Hybrid threats as a concept*, available at: https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/ (accessed 31 March 2026)).

[5] Disinformation can be defined as false or manipulated information deliberately spread with the intent to influence public opinion and cause harm to specific actors (such as groups of people or States) or to more abstract concepts such as democracy, public trust in independent journalism or health care (*see e.g.* European Commission, *A multi-dimensional approach to disinformation: Report of the independent high level group on fake news and online disinformation*, March 2018, available at: https://digital-strategy.ec.europa.eu/en/library/final-report-high-level-expert-group-fake-news-and-online-disinformation, p. 5; C. Wardle, H. Derakhshan, *Information Disorder Toward an interdisciplinary framework for research and policymaking*, Council of Europe Report DGI(2017)09, 27 September 2017, available at: https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c, p. 20; K. Bontcheva, J. Posetti (eds.), *Balancing Act: Countering Digital Disinformation While Respecting Freedom of Expression*, September 2020, available at: https://unesdoc.unesco.org/ark:/48223/pf0000379015 (all accessed 31 March 2026), pp. 3 and 25).

[6] A "cyberattack" is understood herein as a "deliberate, unauthorised insertion of […] computer code into software-operated machines in order to accomplish the tasks the programmer engineered the

international law should be shaped in future to safeguard the international rule of law and help democratic societies remain resilient against attacks from totalitarian regimes. To this end, this article is divided into two parts. The first suggests that while international law remains applicable, its existing structures and doctrines are strained by the nature of the security challenges that Europe currently faces, necessitating proper adjustments. The second proposes three changes that scholars should consider for further discussion and that could render international law more adequate in times when hybrid threats are becoming the primary means of conflict between States.

While this essay focuses on examples of hybrid threats employed by Russia against EU and NATO Member States, one has to note that other parts of the world are also targeted by similar non-conventional threats, including Taiwan, Latin America, and the Middle East and North Africa (MENA).[7] But despite such security threats being a genuinely global phenomenon, in Latin America and MENA, they are largely driven by cybercrime, with elements of malicious operations emerging but less systematically documented. On the other hand, hybrid operations against NATO and EU Member States are not only well-coordinated, but also employed with a strategic objective of undermining the rule of law and democratic resilience. That is why the European perspective is unique, due to the large number and variety of disruptive operations, their everyday character and the fact that mostly all of them originate from one state actor: Russia.

1. NEITHER PEACE NOR WAR – WHAT DOES IT MEAN FOR INTERNATIONAL LAW?

Under international law, it is clear which legal rules apply to peaceful relations between States and which (namely, international humanitarian law) apply in the event of an international armed conflict (IAC).

In general, there are two definitions of an IAC: on the one hand, some States and scholars define it as a confrontation between the armed forces of two or more

code to perform" (D.P. Fidler, *Cyberattacks and international human rights law*, in: S. Casey-Maslen (ed.), *Weapons under International Human Rights Law*, Oxford University Press, Oxford: 2014, p. 303).

[7] *See e.g. Hybrid threat activity in the MENA region: State and non-state actors seeking status and expanding influence*, Hybrid CoE Research Report 5, March 2022, available at: https://www.hybridcoe.fi/wp-content/uploads/2022/03/20220316-Hybrid-CoE-Research-Report-5-Hybrid-threats-MENA-web.pdf; J. Aukia, *China's hybrid influence in Taiwan: Non-state actors and policy responses*, Hybrid CoE Research Report 9, April 2023, available at: https://www.hybridcoe.fi/wp-content/uploads/2023/04/20230406-Hybrid-CoE-Research-Report-9-Chinas-hybrid-influence-in-Taiwan-WEB.pdf (both accessed 31 March 2026).

States;[8] on the other hand, IAC is described as any use of force by one State against another.[9] If one assumes that the first of these variants is proper, the current toll of Russian actions against EU and NATO Member States cannot be described as an IAC until Russian tanks and infantry step into the territory of Poland, the Baltic States, Finland, etc. The second definition appears more promising for describing the current state of Russian actions, though not without problems. In the past, State representatives described certain hybrid operations as a "use of force". When making a statement on the response of the Russian government to the attempted assassination of Sergei and Yulia Skripal in Salisbury in March 2018, UK Prime Minister Theresa May said that the incident "represents an unlawful use of force by the Russian state against the United Kingdom."[10] In the middle of the migration crisis on the Polish–Belarusian border, the Polish government spoke about "unprecedented aggression of Belarus against Poland and the whole European Union."[11]

Such statements, however, are very rare. In November 2025, two individuals working on the commission of the Russian intelligence service detonated explosives on a section of the railway line in central Poland.[12] Fortunately, the gap in the rail-

[8] *See e.g.,* E. Crawford, *Armed Conflict, International*, in: *Max Planck Encyclopedia of International Law*, available at: https://opil.ouplaw.com/display/10.1093/law:epil/9780199231690/law-9780199231690-e429?prd=EPIL, para. 2; D. Schindler, *The Different Types of Armed Conflicts According to the Geneva Conventions and Protocols*, 163-II Recueil des Cours 117 (1979), p. 131; *Manual of Armed Forces Law, Volume 4: Law of Armed Conflict*, available at: https://www.nzdf.mil.nz/assets/Uploads/DocumentLibrary/DM-69-2ed-vol4.pdf (both accessed 31 March 2026), para. 5.2.9.

[9] *See e.g., Article 2,* in: *Commentary on the Third Geneva Convention: Convention (III) Relative to the Treatment of Prisoners of War*, Cambridge University Press, Cambridge: 2021, pp. 92–93; M. E. O'Connell, *Defining Armed Conflict,* 13(3) Journal of Conflict & Security Law 393 (2008), pp. 397–398; ICTY, *Prosecutor v. Tadić*, Appeal on Jurisdiction, No. IT–94–1–AR72, 2 October 1995, para. 70; C. Greenwood, *Scope of Application of Humanitarian Law*, in: D. Fleck (ed.), *The Handbook of International Humanitarian Law*, Oxford University Press, Oxford: 2008, p. 46; H.-P. Gasser, *International Humanitarian Law: an Introduction*, in: H. Haug (ed.), *Humanity For All: The International Red Cross and Red Crescent Movement*, Paul Haupt Publishers Berne, Stuttgart/Vienna 1993, pp. 510–511; *Law of Armed Conflict - Manual*, Joint Service Regulation (Zdv) 15/2, available at: https://www.bmvg.de/resource/blob/93610/ae27428ce99dfa6bbd8897c269e7d214/b-02-02-10-download-manual-law-of-armed-conflict-data.pdf, para. 203; *Manual of the Law of Armed Conflict*, available at: https://usnwc.libguides.com/ld.php?content_id=47416967 (both accessed 31 March 2026), para. 1.33.

[10] *PM Commons statement on Salisbury incident response*, 14 March 2018, available at: https://www.gov.uk/government/speeches/pm-commons-statement-on-salisbury-incident-response-14-march-2018 (accessed 10 January 2026).

[11] *Belarusian hybrid attack on the EU*, 9 November 2021, available at: https://www.gov.pl/web/sluzby-specjalne/belarusian-hybrid-attack-on-the-eu (accessed 31 March 2026).

[12] A. Easton, J. Lukiv, *Two Ukrainians working for Russia behind rail sabotage, Polish PM says*, BBC, 18 November 2025, available at: https://www.bbc.com/news/articles/c4gknv8nxlzo; S. Walker, J. Krupa, *Poland railway blast was unprecedented act of sabotage, says Donald Tusk*, The Guardian, 17 November 2025, available at: https://www.theguardian.com/world/2025/nov/17/poland-railway-blast-was-unprecedented-act-of-sabotage-says-donald-tusk (both accessed 31 March 2026).

way track was detected in time; otherwise, it could have been catastrophic if a train travelling on that line at full speed had derailed. Polish representatives spoke then "only" of acts of sabotage and did not claim that the incident amounted to a violation of the prohibition of the use of force.[13] In fact, how should the destruction of a small part of the railway infrastructure in one State, conducted on the order of another, which could have caused a train derailment but ultimately did not, be qualified from the perspective of international law? Regardless of the different options that may be explored, it seems that labelling such an operation as the use of force would not be justified.

Likewise, one can mention here various cyberoperations conducted by Russia. According to Microsoft's Digital Defense Report 2025, "[o]utside of Ukraine, the top ten countries most affected by Russian cyber activity all belong to NATO – a 25% increase compared to last year."[14] Just to name some of the most recent developments, Russia-related hackers conducted cyberoperations against Belgium,[15] Finland,[16] Poland[17] and the UK.[18] Although the attacks targeted energy infrastructure, health care organisations and websites of the State's organs, among other things, neither of the affected States characterised them as a violation of the prohibition on the use of force. Even though such a legal qualification is theoretically possible, neither of these cases seems to fulfil its criteria, due to the fact that a "cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force."[19] That in turn requires taking into account a number of factors such as "consequences involving physical harm

[13] *Speech by Deputy Prime Minister and Minister of Foreign Affairs Radosław Sikorski in the Sejm*, 19 November 2025, available at: https://www.gov.pl/web/diplomacy/speech-by-deputy-prime-minister-and-minister-of-foreign-affairs-radoslaw-sikorski-in-the-sejm; *PM Tusk in Parliament: Russia Behind Sabotage Attacks in Poland*, 18 November 2025, available at: https://www.gov.pl/web/primeminister/pm-tusk-in-parliament-russia-behind-sabotage-attacks-in-poland (both accessed 31 March 2026).

[14] *Microsoft Digital Defense Report 2025*, available at: https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/msc/documents/presentations/CSR/Microsoft-Digital-Defense-Report-2025.pdf#page=1 (accessed 31 March 2026), p. 47.

[15] *Pro-Russian hackers targeted Belgian government institutions ahead of European summit*, Belga News Agency, 19 December 2025, available at: https://www.belganewsagency.eu/pro-russian-hackers-targeted-belgian-government-institutions-ahead-of-european-summit (accessed 31 March 2026).

[16] *Yle: Russian hacker group targets Finnish government in cyberattacks*, Helsinki Times, 25 September 2025, available at: https://www.helsinkitimes.fi/finland/finland-news/domestic/28002-yle-russian-hacker-group-targets-finnish-government-in-cyberattacks.html (accessed 31 March 2026).

[17] *Poland Stops Cyberattacks on Energy Infrastructure*, 15 January 2026, available at: https://www.gov.pl/web/primeminister/poland-stops-cyberattacks-on-energy-infrastructure (accessed 31 March 2026).

[18] *Rachel Reeves: Russia behind some of recent UK cyber attacks*, ITV, 23 September 2025, available at: https://www.itv.com/news/2025-09-22/rachel-reeves-russia-behind-some-of-recent-uk-cyberattacks (accessed 31 March 2026).

[19] M.N. Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, Cambridge: 2017, p. 330.

to individuals or property",[20] the "immediate results" of the cyber operation,[21] the "degree to which cyber operations intrude into the target State or its cyber systems contrary to the interests of that State",[22] the possibility of evaluating the cyber operation through specific metrics such as the amount of data corrupted, the percentage of servers disabled, etc.[23] or "[t]he extent of State involvement in a cyber operation."[24] Although some of these conditions have been fulfilled in the cases mentioned above (e.g. some cyberoperations targeted a domain name of a particular State or a particular State organ),[25] their severity and invasiveness were limited and some were carried out by groups whose actions would be difficult to attribute to the Russian Federation.

Thus, whether one assumes that armed conflict involves a clash between the armed forces of two States or any use of force, in the legal sense there is no ongoing IAC between any EU or NATO member and Russia. But does this mean that Europe is living in peaceful times? That would not be true either. Attempts to derail trains, parcels exploding at logistics depots,[26] swarms of drones carrying explosives and violating airspace,[27] balloons flying over civilian airports[28] or arson attacks on shopping centres[29] do not precisely match the vision of peace. On the contrary, such a reality forces State organs to change their regular modes of operation, reorganise their structures or submit proposals for changes in the law to respond appropriately and in a timely manner to the constantly emerging threats to the State's security.[30] At the same time, such acts of sabotage prompt fear among societies and begin

[20] *Ibidem*, p. 334.

[21] *Ibidem.*

[22] *Ibidem*.

[23] *Ibidem*, p. 335.

[24] *Ibidem*, p. 336.

[25] *Ibidem*, p. 335.

[26] *Exploding parcels in Europe part of plot to target US flights, officials say*, Euroactive, 31 July 2025, available at: https://www.euractiv.com/news/exploding-parcels-in-europe-part-of-plot-to-target-us-flights-officials-say/ (accessed 31 March 2026).

[27] *Airspace Violation Repelled: Poland's Procedures Prove Effective*, 10 September 2025, available at: https://www.gov.pl/web/primeminister/airspace-violation-repelled-polands-procedures-prove-effective (accessed 31 March 2026).

[28] P. Kirby, *Lithuania declares emergency situation over Belarus balloons*, BBC, 9 December 2025, available at: https://www.bbc.com/news/articles/c39pr3d10wlo (accessed 31 March 2026).

[29] J. Whitehead, *Poland accuses Russia of arson over 2024 shopping centre fire*, BBC, 12 May 2025, available at: https://www.bbc.com/news/articles/cgegj1rvq84o (accessed 31 March 2026).

[30] *See e.g.*, K. Krasuski, Z. Wanat, *Polish Lawmakers Fail to Overturn Veto on Crypto Assets Bill*, Bloomberg, 5 December 2025, available at: https://www.bloomberg.com/news/articles/2025-12-05/polish-lawmakers-fail-to-overturn-veto-on-crypto-assets-bill?embedded-checkout=true; A. Sytas, *Lithuania declares state of emergency over balloons from Belarus*, BBC, 9 December 2025, available at: https://www.reuters.com/world/lithuania-declares-state-emergency-over-smuggler-balloons-belarus-2025-12-09/ (both accessed 31 March 2026).

to influence individuals' everyday life choices.[31] If the threat of further unpredictable attacks begins to guide the judgments of governments and ordinary people, then the term "neither peace nor war" becomes an accurate description of the new reality.

These and similar phenomena are not new; their origins can be traced back to antiquity.[32] It is also difficult to claim that modern international law has not had sufficient time to develop appropriate legal norms and resilience mechanisms to address disinformation, espionage and different acts of sabotage, as such techniques were standard during the Cold War and part of the Soviet Union's arsenal. And yet, the dichotomy between peace and an IAC was sufficient to describe the rights and obligations of States just three decades ago. One could then ask what has changed and how the situation differs today from that faced by States in the recent past. The answer to such a question is undoubtedly complex and would require a proper analysis of multiple political, economic and historical factors. From an international law perspective, though, the most significant change appears to be the technological shift. Thirty years ago, individuals could not have been recruited for sabotage acts via encrypted messaging apps and paid in bitcoin by patrons living thousands of kilometres away; swarms of drones were not flying over the airports in a situation where planes are the everyday means of transport for millions of people; and well-coordinated campaigns of posts spread with the skilful use of social media algorithms could not have influenced the outcome of democratic elections. In other words, technology has changed the world, as have the threats the international community faces. What has not changed is international law.

2. THREE CHANGES TO BE CONSIDERED

It would be unrealistic to propose revising the UN Charter, amending existing treaties or creating a brand-new international organisation that would directly address all the threats contributing to a state of "neither peace nor war", as reforms of the current framework of collective security were attempted in the past, and they proved unsuccessful.[33] Instead, the aim of this essay is to propose initiating a debate among

[31] *Speech by President von der Leyen at the European Parliament plenary debate on a united response to recent Russian violations of the EU Member states' airspace and critical infrastructure*, 8 October 2025, available at: https://ec.europa.eu/commission/presscorner/detail/en/speech_25_2316 (accessed 31 March 2026).

[32] *See e.g.*, J. Lacey, *Conquering Germania: A Province Too Far*, in: W. Murray, P. R. Mansoor (eds.), *Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present*, Cambridge University Press, Cambridge: 2012, pp. 18–44.

[33] *See e.g.* B. Fassbender, *All Illusions Shattered? Looking Back on a Decade of Failed Attempts to Reform the UN Security Council*, 7 Max Planck Yearbook of the United Nations Law 183 (2003); S. Ches-

scholars on introducing a set of changes in international law that would make it more resilient in a "neither peace nor war" situation.

The proposal to recognise a middle state between peace and IAC is not entirely new; since the emergence of the prohibition on the use of force, international law scholars have long debated the existence of a state of "non-belligerency". Before the emergence of the prohibition, when war was a universally admissible means of waging disputes, every State had the right to resort to force for whatever reason. Thus, the statuses of a State that attacked first and one that was only defending itself were equal in the eyes of the law,[34] as neither of them violated legal norms by using forcible measures. That is where the prohibition of the use of force introduced a fundamental change: it prompted the differentiation of belligerents into wrongdoers, i.e. those who attacked first, violating the prohibition of the use of force, and victims, i.e. States which were forced to defend themselves against an illegal attack.[35] As some scholars claim, this change had to affect the strict distinction between neutrality and belligerency, since the prohibition of the use of force permits States to take a stand against the wrongdoer and to help the victim of the illegal use of force.[36] This is the essence of "non-belligerency":[37] non-belligerent States are supposedly allowed to deviate from the core obligations of neutrality – abstention, prevention and impartiality – in order to help the victim of the illegal use of force without becoming a party to an armed conflict.[38] It is true that the legal scholarship does not unanimously agree on the existence and exact scope of non-belligerency as a third category between being a co-belligerent and remaining neutral; there is also hardly any evidence that non-belligerency is supported by treaties or customary law.[39]

---

terman, *Untied Nations? Saving the UN Security Council*, 36(4) European Journal of International Law 1089 (2025).

[34] M.N. Schmitt, *Providing Arms And Materiel To Ukraine: Neutrality, Co-Belligerency, And The Use Of Force*, Articles of War, 7 March 2022, available at: https://lieber.westpoint.edu/ukraine-neutrality-co-belligerency-use-of-force/ (accessed 31 March 2026).

[35] *Ibidem.*

[36] *See* S.A.G. Talmon, *The Provision of Arms to the Victim of Armed Aggression: the Case of Ukraine (April 6, 2022)*, 20 Bonn Research Papers on Public International Law 1 (2022), pp. 18–19, 21.

[37] *See e.g.* T. Komarnicki, *The Place Of Neutrality in the Modern System Of International Law*, 80 Recueil des cours 395 (1952), p. 482; M. Bothe, *The Law of Neutrality*, in: D. Fleck (ed.), *The Handbook of International Humanitarian Law*, Oxford University Press, Oxford: 2008, p. 573; A. Gioia, *Neutrality and Non-belligerency*, in: H.H.G. Post (ed.), *International Economic Law and Armed Conflict*, Martinus Nijhoff Publishers, Dordrecht/Boston/London: 1994, pp. 66–67; D. W. Bowett, *Self-defence in International Law*, The Lawbook Exchange, Clark, NJ: 2009, pp. 174–175; R. Ingber, *Co-Belligerency*, 42 The Yale Journal of International Law 67 (2017), p. 89.

[38] N. Ronzitti, *Italy's Non-Belligerency During The Iraqi War*, in: M. Ragazzi (ed.), *International Responsibility Today*, Martinus Nijhoff Publishers, Leiden/Boston: 2005, p. 198.

[39] A. Kleczkowska, *Neutrality, Non-belligerency, Belligerency: The Status of states Assisting Ukraine in the International Armed Conflict between Ukraine and Russia*, in: M. Balcerzak, E. Cała-Wacinkiewicz

However, the mere fact that both States and scholars are discussing the possibility of a legal status for such a position indicates that new developments in security can stimulate such debates, even if, at first, these discussions remain an intellectual exercise and do not take the form of firm legislative proposals.

The three changes proposed for international law scholars to consider, described below, were selected because they relate to three important aspects of non-conventional threats: legal qualification of such threats as violations of international law; ensuring the safety of ordinary citizens amid everyday hybrid operations; and the possibility of effectively and instantly responding to hybrid threats in line with international law. One could certainly enumerate many more legal questions to be addressed, particularly the problem of attributing violations of international law to a specific State in order to hold it responsible. To attribute certain violations of international legal norms to Russia, such violations must have been committed either by State organs or a person or entity which is empowered by Russian law to exercise elements of governmental authority or which is acting on Russia's instructions or under its direction or control.[40] Russia, however, often utilises various non-state actors who, despite financial, political, organisational or familial ties to Russian State organs, do not fit into any of those definitions, making it impossible to attribute certain actions to Russia in a legal sense.[41] On the one hand, the question of attribution is therefore not only a legal question, but also a matter of gathering factual evidence of the connections between different actors and Russia; on the other hand, it is secondary to the problem of Russia's violations of international law, because if certain conduct cannot be labelled as a breach of law, there will be no need to further consider attribution. From this perspective, the three proposed changes are not only more feasible to implement and directly connected to legal considerations, but also require an urgent response, given the challenges they pose to societal resilience. In a broader sense, the discussion of those issues can serve as a model for how to proceed and search for relevant legal solutions to additional questions which may arise.

Firstly, States should agree on a new approach to coercion as an element of the principle of non-intervention. In general, coercion may be defined as an act designed

(eds.), *Legal Perspectives on the Russia-Ukraine War: International and Polish Approaches*, Routledge, New York/London: 2025, pp. 20–29.

[40] International Law Commission, Responsibility of States for Internationally Wrongful Acts, II (Part Two) Yearbook of the International Law Commission (2001), Arts. 4–5, 8.

[41] *See e.g.* E. Volāns et al., *Handbook on the role of non-state actors in Russian hybrid threats*, Hybrid CoE Paper 27, December 2025, available at: https://www.hybridcoe.fi/wp-content/uploads/2025/12/Hybrid-CoE-Paper-27-Handbook-on-the-role-of-non-state-actors-in-Russian-hybrid-threats.pdf (accessed 31 March 2026).

to deprive another State of its freedom of choice.[42] Traditionally, scholars have distinguished two forms of coercion: firstly, there is "dictatorial" coercion, which consists of "compelling another State to do or not to do something."[43] It involves issuing a demand that is backed by a threat, meaning an explicit or implicit promise of harm whose execution depends on whether the target State fulfils the demanded conditions.[44] The second form is "forcible" coercion, or "taking control of a certain matter and forcibly imposing a condition of things."[45] In other words, "the intervening state replaces the will of the victim state with its own by carrying out the unauthorized act itself instead of pressuring someone else to do anything."[46] Given these descriptions of coercion, the majority of hybrid operations undertaken by one State against another cannot be classified as coercion. When it comes to disinformation campaigns aimed at meddling in the electoral process, for example, in order for them to be labelled as a violation of the principle of non-intervention, they would have to be accompanied by either a threat whose aim would be to compel a State to call a specific election result, or the foreign State taking control of all media outlets and official sources of information about candidates and elections, depriving voters of independent sources of information in order to manipulate them into supporting a specific candidate.[47] Consequently, such a definition of coercion would not include, for example, using thousands of fake accounts on an

[42] *Costa Rica's Position on the Application of International Law in Cyberspace*, available at: https://tinyurl.com/mw99u3jb (accessed 31 March 2026), para. 24; Schmitt, *supra* note 19, p. 317, para. 18.

[43] L. Oppenheim, *International Law: A Treatise*, vol. 1, Longmans, Green and Co., London/New York: 1905, p. 181; M. Roscini, *International Law and the Principle of Non-Intervention: History, Theory, and Interactions with Other Principles*, Oxford University Press, Oxford: 2024, p. 152; M. Milanovic, *Revisiting Coercion as an Element of Prohibited Intervention in International Law*, 117(4) The American Journal of International Law 601 (2023), p. 605; X.W. Tay, *Reconstructing the Principle of Non-Intervention and Non-Interference-Electoral Disinformation, Nicaragua, and the Quilt Work Approach*, 40 Berkeley Journal of International Law 39 (2020), p. 46; Q. Rolando, *Diritto Internazionale Pubblico*, G. Priullla Editore, Palermo: 1956, p. 216; *International Law in Future Frontiers*, 19 May 2022, available at: https://www.gov.uk/government/speeches/international-law-in-future-frontiers; UNGA, *Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by states submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*, established pursuant to General Assembly Resolution 73/266, 13 July 2021, UN Doc. A/76/136, p. 57; *The Application of International Law to State Activity in Cyberspace*, available at: https://tinyurl.com/mvhrht5k (both accessed 31 March 2026), para. 9.

[44] Roscini, *supra* note 43, p. 153.

[45] *Ibidem,* p. 152. *See also* Milanovic, *supra* note 43, p. 605.

[46] Roscini, *supra* note 43, p. 155.

[47] *See e.g.* M.N. Schmitt, *Foreign Cyber Interference in Elections: An International Law Primer, Part I*, EJIL:Talk!, 16 October 2020, available at: https://www.ejiltalk.org/foreign-cyber-interference-in-elections-an-international-law-primer-part-i/ (accessed 31 March 2026). *See also* J.D. Ohlin, *A Roadmap for Fighting Election Interference*, 115 AJIL Unbound 69 (2021), p. 70.

online platform or spreading propaganda in support of specific candidates through a media outlet that is overtly or covertly sponsored by a foreign State.

It is important to note that international law scholars have proposed advocating for a broader, more flexible approach to the notion of coercion in cases of disinformation. These proposals suggest that the determination of "coercion" should consider a range of factors, such as which values were affected by the outcome of the disinformation campaign, how many individuals were impacted and to what extent was the freedom to act and make certain choices constrained due to the lack of accurate information.[48] Moreover, some States have endorsed such a qualification of disinformation, including in their positions on applying international law to cyberspace.[49]

Even though it is much too early to conclude this brief analysis by saying that there is consensus among States that coercion is not limited only to "dictatorial" or "forcible" conduct, the discussion about disinformation and the principle of non-intervention may serve as an example of how gradually the new security threats may contribute to changing the interpretation of fundamental principles of international law. Thus, if it is possible with respect to one type of hybrid threat, legal scholars should also initiate similar discussions regarding other operations, and should encourage States

[48] M.S. McDougal, F.P. Feliciano, *International Coercion and World Public Order: The General Principles of the Law of War*, 67 Yale Law Journal 771 (1958), pp. 781–782; B. Sander, *Democracy Under The Influence: Paradigms of state Responsibility for Cyber Influence Operations on Elections*, 18(1) Chinese Journal of International Law 1 (2019), pp. 22–23; B. Baade, *Fake News and International Law*, 29(4) European Journal of International Law 1357 (2018), p. 1364; S. Wheatley, *Foreign Interference in Elections under the Non-intervention Principle: We Need to Talk about "Coercion"*, 31 Duke Journal of Comparative & International Law 161 (2020), pp. 191–192; A. Rotondo, P. Salvati, *Fake News, (Dis)information, and the Principle of Nonintervention: Scope, limits, and possible responses to cyber election interference in times of competition*, The Cyber Defense Review 209 (2019), pp. 211–212; W. Ossoff, *Hacking the Domaine Réservé: The Rule of Non-Intervention and Political Interference in Cyberspace*, 62(1) Harvard International Law Journal 296 (2021), p. 309; M.N. Schmitt, *"Virtual" Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law*, 19(1) Chicago Journal of International Law 30 (2018), p. 51; N. Tsagourias, *Electoral Cyber Interference, Self-Determination and the Principle of Non-Intervention in Cyberspace*, EJIL: Talk!, 26 August 2019, available at: https://www.ejiltalk.org/electoral-cyber-interference-self-determination-and-the-principle-of-non-intervention-in-cyberspace/ (accessed 31 March 2026).

[49] *See e.g. Costa Rica's Position on the Application of International Law in Cyberspace*, *supra* note 42, para. 25; UN Doc. A/76/136, *supra* note 43, pp. 34–35; *General Staff of Iranian Armed Forces Warns of Tough Reaction to Any Cyber Threat*, Nournews, 18 August 2020, available at: https://nournews.ir/En/News/53144/General-Staff-of-Iranian-Armed-Forces-Warns-ofTough-Reaction-to-Any-Cyber-Threat; *Application of International Law to State Activity in Cyberspace*, *supra* note 43, para. 10; The Republic of Poland's position on the application of international law in cyberspace, 19 December 2022, available at: https://www.gov.pl/web/diplomacy/the-republic-of-polands-position-on-the-application-of-international-law-in-cyberspace (both accessed 31 March 2026), p. 4; UNGA Verbatim Record, 1st Committee, 7 December 1965, UN Doc. A/C.1/SR.1399, para. 11; UNGA Verbatim Record, 1st Committee, 7 December 1965, UN Doc. A/C.1/SR.1398, para. 29; UNGA Verbatim Record, 1st Committee, 3 December 1965, UN Doc. A/C.1/SR.1395, para. 23; UNGA Verbatim Record, 1st Committee, 8 December 1965, UN Doc. A/C.1/SR.1402, para. 24.

to participate in that debate. The positive outcome of such a discussion could possibly have enormous significance, as it could enable the qualification of at least some hybrid threats as violations of the principle of non-intervention and, thus, of international law.

Secondly, States should agree that no hybrid operation may infringe on fundamental standards of humanity. This phrase is used after Resolution 1998/29 of the Commission on Human Rights[50] and the Analytical Report of the Secretary-General submitted pursuant to Commission on Human Rights Resolution 1997/21; and it is a successor to the term "minimum humanitarian standards".[51] "Fundamental standards of humanity" would not only include the standards of international human rights law and international humanitarian law, but would also recognise that "in cases not covered by human rights and humanitarian instruments, all persons and groups remain under the protection of the principles of international law derived from established custom, from the principles of humanity and the dictates of public conscience."[52] These latter two terms refer to the Martens Clause,[53] and despite their vagueness they are introduced here intentionally. In the Martens Clause, the precise content of "the laws of humanity, and the requirements of the public conscience" was left "to be ascertained in the light of changing conditions, inclusive of changes in the means and methods of warfare and the outlook and tolerance levels of the international community."[54] That is also why these two terms are well-suited to the context of hybrid threats, where tactics and modes of operation constantly change.

What would these fundamental standards of humanity mean in practice? They would oblige States to, for example, not conduct hybrid operations in a manner that affects individuals who are not members of the military, law enforcement or other organs responsible for State security.[55] This is not to say that drones flying over a nuclear submarine base[56] are acceptable, but that militaries and law enforcement

[50] Commission on Human Rights Resolution 1998/29, 17 April 1998, para. 1.

[51] The term "minimum humanitarian standards" was criticised for a number of reasons. *See* UN Economic and Social Council, Minimum humanitarian standards: Analytical report of the Secretary-General submitted pursuant to Commission on Human Rights resolution 1997/21, 5 January 1998, UN Doc. E/CN.4/1998/87, para. 5; UN Economic and Social Council, Minimum humanitarian standards: Report of the Secretary-General, 28 January 1997, UN Doc. E/CN.4/1997/77/Add.1, paras. 47, 54.

[52] *Declaration of Minimum Humanitarian Standards*, 2 December 1990, available at: https://www.ifrc.org/Docs/idrl/I149EN.pdf (accessed 31 March 2026), preamble.

[53] *See e.g.* Convention (II) with respect to the Laws and Customs of War on Land, in: J. Brown Scott (ed.), *The Hague Conventions and Declarations of 1899 and 1907*, Oxford University Press, London: 1915, pp. 101–102.

[54] Dissenting Opinion of Judge Shahabuddeen in ICJ, *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion, 8 July 1996, ICJ Rep 1996, p. 406.

[55] The proposals on what "fundamental standards of humanity" mean in practice come from the modified *Declaration of Minimum Humanitarian Standards Adopted, supra* note 52.

[56] *France takes anti-drone measures after flight over nuclear submarine base*, France 24, 5 December 20025, available at: https://www.france24.com/en/live-news/20251205-france-takes-anti-drone-meas-

officers are trained and equipped to deal with such threats, as opposed to ordinary citizens. Next, "[w]eapons or other material or methods prohibited in international armed conflicts must not be employed in any circumstances."[57] Also, "[a]cts or threats of violence the primary purpose or foreseeable effect of which is to spread terror among the population are prohibited."[58] Medical and religious personnel and objects must be respected and protected.[59] In other words, fundamental standards of humanity would prohibit attacking passenger trains, civilian airports or shopping centres; putting into circulation packages with incendiary devices,[60] or tampering with critical infrastructure – including power stations and waterworks – in a way that could affect the safety and well-being of individuals.[61]

One may ask whether existing international law already protects the persons and objects enumerated above, rendering this proposal unnecessary. The answer, in the context of hybrid operations, is that it does not – or at least not effectively. International human rights law, while guaranteeing the right to life and physical integrity, is of limited application in cases such as those described above. This is because States primarily owe obligations to all individuals on their territory and subject to their jurisdiction.[62] Therefore, Russia cannot be held responsible for violations of the right to life as a result of the acts of sabotage committed by its proxies in Estonia, Lithuania or Poland. And while there has been growing acceptance that human rights obligations are also applicable extraterritorially[63] when the State exercises power or effective control over an individual or when an individual is in an area subject to the State's control,[64] neither of these conditions is true in the cases under consideration. Likewise, despite international humanitarian law requiring that civilians be distinguished

ures-after-flight-over-nuclear-sub-base (accessed 31 March 2026).

[57] *Declaration of Minimum Humanitarian Standards*, Art. 5(3).

[58] *Ibidem*, Art. 6.

[59] *Ibidem*, Art. 14.

[60] G. Blackburn, *Poland detains eight over suspected Russia-linked sabotage, says PM Tusk*, Euronews, 21 October 2025, available at: https://www.euronews.com/2025/10/21/poland-detains-eight-over-suspected-russia-linked-sabotage-says-pm-tusk (accessed 31 March 2026).

[61] B. Żurawicz, *Wtargnęli na teren stacji uzdatniania wody. "Ingerencja w najważniejsze obiekty"* [They broke into the water treatment plant. "Interference with key facilities"], TVN24, 16 September 2025, available at: https://tvn24.pl/krakow/krakow-intruzi-na-terenie-wodociagow-dwie-osoby-zatrzymane-st8652190 (accessed 31 March 2026).

[62] *See* Art. 2(1) of the International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976), 999 UNTS 171. *See also* UNCHR, *General comment No. 31 [80], The nature of the general legal obligation imposed on States Parties to the Covenant"*, 26 May 2004, CCPR/C/21/Rev.1/Add. 13, para. 10.

[63] M. Milanovic, *Extraterritorial Application of Human Rights Treaties*, Oxford University Press, Oxford: 2011, p. 8.

[64] *Ibidem*, p. 119–173; ECtHR, *Banković and others v. Belgium and Others* (App. No. 52207/99), 12 December 2021, para. 7.

from combatants,[65] prohibiting attacks that target civilians or civilian objects[66] and banning the use of weapons which are by nature indiscriminate,[67] it is not applicable to the cases described herein, since – as argued above – no IAC exists between Russia and NATO/EU Member States. Thus, the result is a genuine normative gap: conduct that threatens civilian safety and well-being, when executed through hybrid means below the threshold of IAC and outside the reach of extraterritorial human rights jurisdiction, may go unaddressed by any primary rule of international law.

The legal status of fundamental standards of humanity would be the main challenge. Needless to say, the most effective way of implementing the standards would be through a customary norm. On the one hand, all States would be bound by, and eventually held responsible for, noncompliance with such a norm. On the other hand, being unwritten, the norm would remain flexible and responsive in the event of new threats or modes of operation emerging. However, there is one, albeit significant, problem with fundamental standards of humanity – what conduct would it exactly require from States? Thus, the same issue as with the Martens Clause reoccurs here: "the laws of humanity, and the requirements of the public conscience" are too broad and vague to form the basis of a State's obligation.[68] Moreover, despite the fundamental standards of humanity or minimum humanitarian standards applicable to situations beyond armed conflicts having been long discussed by States, it remains doubtful that they have attained the status of a customary norm.[69] This should not lead to the conclusion, however, that these standards are without legal significance or that they should be abandoned. Given the genuine normative gap identified above – where hybrid operations that threaten civilian safety and well-being escape the reach of both international humanitarian law and international human rights law – the need for a governing primary rule is not merely theoretical, but urgent. States committed to the rules-based international order should not treat the standard as a distant aspiration, but should work to create the contours of the emerging norm.

Thirdly, States need to be equipped with more effective means for reacting to hybrid threats. Today, the most common means of responding to arson or attacks

[65] Arts. 48, 51(2) and 52(2) of the Protocol additional to the Geneva Conventions of 12 August 1949, and relating to the protection of victims of international armed conflicts (Protocol I) (adopted 8 June 1977, entered into force 7 December 1978), 1125 UNTS 3.

[66] *Ibidem*.

[67] *Ibidem*, Art. 51(4).

[68] E. Crawford, *The Modern Relevance of the Martens Clause*, 6 ISIL Yearbook of International Humanitarian and Refugee Law 1 (2006), p. 21.

[69] *Declaration of Minimum Humanitarian Standards (1990): Introduction by Asbjørn Eide and Allan Rosas (1997)*, available at: https://www.abo.fi/wp-content/uploads/2018/03/IMR-Declaration-of-minimum-standards-web-2018.pdf (accessed 31 March 2026), pp. 1–5.

on critical infrastructure are retorsions, which are unfriendly but legal measures. Although they are adequate to express frustration regarding various hybrid operations, they are usually insufficient to induce compliance with international law or deter future actions.

Another unilateral tool available to States is countermeasures. Their use, however, is subject to several procedural conditions established in customary law[70] and subsequently listed by the International Law Commission. One of the most problematic steps in the process of applying countermeasures seems to be that, before they are enforced, an injured State must first call upon the responsible State, giving it notice of its claim, in which it has to specify in particular the conduct that the responsible State should take to cease the wrongful act (if it is continuing) and the form of reparation.[71] If the responsible State does not cease the wrongful act or the dispute does not become pending before a court or tribunal which has the authority to make decisions binding on the parties,[72] and the injured State ultimately decides to resort to countermeasures, before taking any such steps, it must first notify the responsible State of such a decision and offer to negotiate with that State.[73] Thus, by providing notice of a claim or notifying the responsible State, the injured State must reveal that it is aware of the wrongful act and that it is preparing a response to that act. In the case of hybrid threats, issuing such notifications to the responsible State before concrete measures are adopted would not only delay the adoption of a proper response, but also deprive the injured State's answer of the element of surprise.

Much stricter requirements for countermeasures than for retorsions are an obvious consequence of the fact that, unlike retorsions, countermeasures comprise measures that violate international law. Thus, all the conditions of legality listed by the International Law Commission are intended to protect the international community from escalation, chaos and abuse caused by the overbroad and reckless use of measures that breach legal norms. The aim of this proposal is not to diminish the importance of these conditions for the legality of countermeasures, but rather to adapt them to the current needs of the international community.

---

[70] *See e.g.* statements on countermeasures presented by States in their positions on the use of international law in cyberspace in Cyber Law Toolkit, *National position*, available at: https://cyberlaw.ccdcoe.org/wiki/Category:National_position (accessed 31 March 2026); Regulation (EU) 2023/2675 of the European Parliament and of the Council of 22 November 2023 on the protection of the Union and its Member states from economic coercion by third countries, [2023] OJ L 1, preambular para. 13.

[71] International Law Commission, *supra* note 40, Art. 43.

[72] *Ibidem*, Art. 52(3).

[73] *Ibidem*, Art. 52(1).

Bearing all this in mind, the international community should consider waiving the obligation to submit the notice of claim and to notify the responsible State of the ultimate decision to undertake countermeasures, or at least to mitigate them to the extent necessary to avoid delaying a proper response. Even without these two steps in the process of employing countermeasures, the remaining conditions of their legality would still prevent countermeasures from becoming an uncontrolled form of revenge against the responsible State. One can consider the following scenario: one State conducts a cyberattack against another, affecting the latter State's critical infrastructure or deeply interfering with its electoral process in a way that changed the outcome of an election. The cyberattack constitutes a violation of international law and can be attributed to the responsible State (i.e., constitutes an internationally wrongful act). In such a case, the injured State is entitled to respond with a countermeasure, including one conducted in cyberspace, even if that response would otherwise amount to a violation of the principles of non-intervention, the right to self-determination, or others. Even if the obligation to submit a notice of claim and to notify the responsible State of the decision to undertake countermeasures were waived, in such a case the countermeasure must still only induce the responsible State to comply with the legal obligations it owes the injured State, must be limited to the non-performance for the time being of international obligations of the State taking the measures towards the responsible State and must be taken in such a way as to permit the resumption of performing the obligations in question. The countermeasure must not violate the prohibition of the threat or use of force, obligations to protect fundamental human rights, obligations of a humanitarian character prohibiting reprisals or other obligations under peremptory norms of general international law. It must also be proportionate and be terminated as soon as the responsible State has complied with its obligations.[74] Moreover, an injured State may take a countermeasure only against a State responsible for an internationally wrongful act, to the exclusion of third States.[75]

One could ask whether broadening the scope of possible uses of unilateral measures would be counterproductive, as it would only reinforce arguments that international law is a primitive system of law based on self-help[76] and, consequently,

[74] *See* International Law Commission, *supra* note 40, Arts. 49-54; Schmitt, *supra* note 19, pp. 111–134.

[75] T. Ruys, *Sanctions, Retorsions and Countermeasures: Concepts and International Legal Framework*, in: L. van den Herik (ed.), *Research Handbook on UN Sanctions and International Law,* Edward Elgar Publishing, Cheltenham: 2016, p. 34.

[76] *See e.g.* M. Noortmann, *Enforcing International Law: From Self-Help to Self-Contained Regimes*, Routledge, London/New York: 2005, p. 2; A. Van Wynen Thomas, A.J. Thomas, Jr., *Non-Intervention: The Law and its Import in the Americas*, Southern Methodist University Press, Dallas: 1956, p. 85; A. Pellet, A. Miron, *Sanctions*, in: *Max Planck Encyclopedias of International Law*, available at: https://opil.ouplaw.com/display/10.1093/law:epil/9780199231690/law-9780199231690-e984 (accessed 31 March 2026),

constitute a regression to such institutions as the collective security system within the UN, which was supposed to protect the international community against unilateral revanchism. However, for some time now, the collective security system – with the UN Security Council at its apex – has not been functioning in accordance with the aims for which it was established. It is a different matter how to reform or replace such broken institutions and organs, but since it does not seem that any such profound reform is possible any time soon, the international community – including international law scholars – should focus on adjusting the viable existing tools available to States to meet the current challenges.

CONCLUSIONS

The aim of this short essay is to initiate a discussion about how international law, and consequently the part of the international community that seeks to safeguard the international rule of law, can become more resilient towards nonconventional threats that States are facing these days. This refers specifically to threats targeting NATO and EU Member States that originate from Russia, collectively termed hybrid threats. These threats affect the functioning of State institutions, pose serious risks to life and to the operation of critical infrastructure and spread fear among societies; nonetheless, they do not constitute an IAC. Moreover, while the atmosphere in Europe can hardly be described as peaceful, peacetime norms continue to apply to such phenomena from an international law perspective. Since defining hybrid threats as a new intermediate state between peace and IAC would be very difficult or even impossible from a legal point of view, this essay proposes three types of changes that could be introduced to the existing legal framework, rendering international law at least a little more resilient in the face of hybrid threats: redefining coercion as an element of the principle of non-intervention, making fundamental standards of humanity applicable to every hybrid operation and waiving the obligations to notify the responsible State as a condition for the legality of countermeasures. There is no doubt that these proposals require further discussion on their details, legal status and scope of application, and hopefully this essay can initiate such a debate.

---

para. 7; J.L. Kunz, *Sanctions in International Law*, 54(2) The American Journal of International Law 324 (1960), p. 325; A. Whelan, *Reciprocity in Public International Law*, Cambridge University Press, Cambridge: 2023, p. 4; L. Fisler Damrosch, *Enforcing International Law Through Non-forcible Measures*, 269 Recueil des Cours 9 (1997), p. 23.