
© Comfreak/Pixabay
THREATS

Thresholds in Cyber and in Space

IV

Lessons Learned from State Positions on the Application of International Law to Cyber for the Evolving Space Domain

By Mr Sebastian Cymutta, Law Researcher
NATO Cooperative Cyber Defence Centre of Excellence

Introduction

On January 17th of 2022, NATO published its 'Overarching Space Policy',[1] laying down the Alliance's understanding and posture with regard to space. This policy document is a direct follow up to the 2021 NATO summit in Brussels and integrated the statement of the summit's communiqué regarding Article 5 of the North Atlantic Treaty[2] with almost identical wording:

'(…) Allies agreed that attacks to, from, or within space present a clear challenge to the security of the Alliance, the impact of which could threaten national and Euro-Atlantic prosperity, security, and stability, and could be as harmful to modern societies as a conventional attack. Such attacks could lead to the invocation of Article 5.'[3]

This part of the communiqué came across as logical, seeing that NATO already declared space as an operational domain in December 2019.[4] Moreover, it mirrors the approach taken by NATO with respect to interference in cyberspace. With regard to cyberspace, the Alliance first clarified the applicability of Article 5 of the North Atlantic Treaty during the 2014 Wales summit[5] before assigning cyberspace the status of an operational domain two years later in Warsaw.[6]

Comparing the declarations of Wales (concerning cyber) and of Brussels (concerning space) with regard to when Article 5 of the North Atlantic Treaty would be activated, the wording is almost identical as well:

'A decision as to when such attacks would lead to the invocation of Article 5 would be taken by the North Atlantic Council on a case-by-case basis.'[7]

While law and policy are sometimes ambiguous, with the prevailing view that international law applies to cyber operations,[8] a robust understanding regarding the operationalization of the cyber domain has emerged.

Even though there is a legal framework for space in existence[9] (which is not the case for cyberspace), some of the most pressing legal issues regarding that domain are identical to those discussed regarding cyber. The most prominent question revolves around the threshold for an 'armed attack' in the sense of Article 51 of the UN-Charter.[10] Closely connected is the question, of when the threshold to a prohibited 'use of force' according to Article 2(4) of the UN-Charter has been crossed.

The Cyber Discourse Regarding 'Thresholds'

These thresholds play an essential part when nations try to fill the above-mentioned 'case-by-case'-paradigms with life.

In July 2021, the United Nations Group of Governmental Experts published an official compendium of voluntary national contributions on how international law applies to the use of information and communication technologies by states.[11] While the comprehensiveness of this compendium is gradually decreasing as more and more nations continue to publish their state positions, these policy documents continue to provide practical solutions for the thresholds of armed attacks and the prohibited use of force.

Use of Force

The concept of the prohibition of the use of force, as it is enshrined in Article 2(4) of the UN-Charter, was shaped by the so-called 'Nicaragua Judgement' of the International Court of Justice (ICJ) in 1986.[12] Here, the ICJ established what has come to be known as the 'scale and effects'-test for determining if a certain state action qualifies as an 'armed attack'[13] while addressing the duality of the concept of 'use of force' in Article 2(4) and 'armed attack' in Article 51.[14]

These considerations still provide guidance today and have been adopted by the Tallinn Manual 2.0[15] to clarify the application and purpose of the prohibition of the use of force regarding cyber operations.[16] Although nations do not endorse them, the rules formulated by the Tallinn Manual 2.0 have nevertheless proven to be very influential[17] in the drafting of state positions.

While the benefit of translating the principles of the 'Nicaragua Judgement' into 'Tallinn Manual rules' for discussing the application of international law to cyber-operations is undeniable, it still leaves room for interpretation. Here, state positions benefit the discourse by commenting on certain situations, clarifying ambiguous legal terms and showcasing scenarios.

For example, the Norwegian State Position published in late 2021 reiterates that Norway would consider inter alia 'cyber-operations leading to the destruction of stockpiles of Covid-19 vaccines, which could amount to the use of force in violation of Article 2(4)'.[18]

Furthermore, there appears to be a growing willingness of states to assume a violation of the prohibition of the use of force by cyber-operations that do not result in physical effects. France is the most outspoken proponent of this view when it 'does not rule out the possibility that a cyber-operation without physical effects may also be characterized as a use of force'.[19]

Armed Attack

While some states would consider the legal effects of the terms 'use of force' and 'armed attack' synonymous[20] most states that have commented on this topic distinguish between the two concepts.

When the Tallinn Manual 2.0 proposed that

'A State that is the target of a cyber-operation that rises to the level of an armed attack may exercise its inherent right to self-defence',[21]

many nations subscribed to this rule,[22] effectively integrating it into their state positions on how international law applies to cyber.

As with the 'use of force threshold', there is a growing tendency to open up the concept of incorporating scenarios which are void of physical effects. For example, when discussing which factors to consider when assessing the effects of a cyber-operation, Germany points out that also 'injury and death (including as an indirect effect)' [23] could be taken into account. France puts forward the idea that even 'considerable economic damage'

could be a deciding factor when appraising the legal consequences of a cyber-attack.[24]

Though not a predetermining factor, many states pointed to the impairment of critical infrastructure as a factor to be considered when assessing the 'scale and effects' of a cyber-operation potentially being categorized as an armed attack.[25]

Implications for the Space Debate

Legal questions regarding the application of international law in space have been discussed quite vividly in the last years. In accordance with Article III Outer Space Treaty, this paper will presume that Article 2(4) and Article 51 of the UN-Charter are applicable in the space domain.[26]

The following paragraphs will explore the implications of the above-mentioned state positions for the legal operationalization of space.

Use of Force

Leaving aside kinetic measures against space infrastructure,[27] it is conceivable that a cyber-attack could affect space assets like satellites and render them inoperable without creating physical damage. As more states are willing to consider attacks void of physical consequences as a use of force,[28] the 'scale and effects'-test needs to be applied to such a scenario.

Space infrastructure provides for many services considered essential today (for example, navigation, communication and banking). Thinking about the reliance of not only the national governments but also of private businesses and citizens, widespread service denials caused by a cyber-

operation adversely affecting the provision of satellite services could easily be considered as breaking the 'use of force threshold'.

Armed Attack

Staying with the picture of a 'threshold', there is a logical step to be taken to consider an attack in the space domain not only a 'use of force' but also as 'armed attack'. That means that the allegorical 'threshold' to an 'armed attack' is actually an instrument to distinguish the scope of application of Article 2(4) and 51 of the UN-Charter from each other while at the same time underlining the interconnectedness of these concepts.

If states are willing to consider non-physical results sufficient for the invocation of Article 5 of the North Atlantic Treaty, the simple fact that almost all western nations are reliant upon space-satellite services is making it more likely that an attack against space infrastructure – whether staged through cyberspace or not – could cross this threshold.

Conclusion

Space has become NATO's 5th distinguished operational domain of warfighting, yet every major mission or operation has to be conducted in a cross-domain setting'.[29]

Hence, it is important not only to think of these domains together but also not to reinvent the wheel with regard to legal issues that have already been addressed in the context of the other domains.

Therefore, the author proposes referring to the lessons learned in the cyber domain to facilitate the evolution of NATO's legal posture in outer space.

Mr Sebastian Cymutta studied law at the University of Münster (Germany) as well as the University of Tartu (Estonia). After passing the German Bar, he started his career as a Legal Counsel with the German Aerospace Centre in Cologne in 2014, before moving on to the German armed forces as a Litigator (2015) and later as a Senior Adviser (2017). As of 2019, he is seconded to the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn (Estonia) as a Law Researcher. There, he focusses on the application of international law to cyber operations as well as to emerging technologies.

Endnotes

1. https://www.nato.int/cps/en/natohq/official_texts_190862.htm; hereafter referred to as 'Overarching Space Policy'.
2. https://www.nato.int/cps/en/natohq/news_185000.htm, para 33.
3. Overarching Space Policy, para 12.
4. https://www.nato.int/cps/en/natohq/official_texts_171584.htm, para 6.
5. https://www.nato.int/cps/en/natohq/official_texts_112964.htm, para 72.
6. https://www.nato.int/cps/en/natohq/official_texts_133169.htm, para 70.
7. Overarching Space Policy, para 12 and for cyber https://www.nato.int/cps/en/natohq/official_texts_112964.htm, see para 72, referring to 'cyber attacks'.
8. This opinion has been emphasized by numerous state position reflecting this point, amongst them Germany, France and Norway, just to name a few.
9. Most notably, the Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies ('Outer Space Treaty').
10. This Article is the key reference in Article 5 of the North Atlantic Treaty.
11. Accessible here: https://www.un.org/disarmament/group-of-governmental-experts/.
12. CASE CONCERNING MILITARY AND PARAMILITARY ACTIVITIES IN AND AGAINST NICARAGUA, Judgement of 27 June 1986, henceforth referred to as the 'Nicaragua Judgement'.
13. Nicaragua Judgement, para 195.
14. Implying, that only the gravest forms of the 'use of force' could be considered an armed attack, effectively putting the two concepts into an escalatory hierarchy, see Nicaragua Judgement, para 191.
15. The Tallinn Manual 2.0 on the International Law applicable to Cyber Operations, Cambridge University Press, 2017.
16. See Tallinn Manual 2.0 rule 69, para 1.
17. See On the Application of International Law in Cyberspace Position Paper – March 2021 (henceforth referred to as the German State Position), available here; https://www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf, which is repeatedly referencing the Tallinn Manual 2.0, e.g. II.a.; II.c.

18. Norwegian positions on selected questions of International Law relating to Cyberspace (henceforth referred to as the Norwegian State Position), para 3.3, see: https://www.regjeringen.no/contentassets/a8911fc020c94eb386a1ec7917bf0d03/norwegian_positions.pdf.
19. See International Law applied to Operations in Cyberspace (henceforth referred to as the French State Position), para 1.1.2; also, the Norwegian State Position is leaning into this direction see footnote 19, para 3.3.
20. The United States of America being the most outspoken proponent of this idea.
21. Tallinn Manual 2.0, rule 71.
22. Expressis verbis German State Position, para IV.b.4; 'Germany concurs with the view expressed in rule 71 of the Tallinn Manual 2.0'.
23. German State Position, para IV.b.4.
24. French State Position, para 1.2.1.
25. Ibid; Norwegian State Position, para 3.3.
26. Häussler, NZWehrr 2020, 221(223).
27. Froehlich, NATO Legal Gazette, 86(95), rightfully argues that these actions should be considered an armed attack.
28. See supra note 19 and 23.
29. For further analysis, see Maj Fotios Kanellos', Defending Space in and through Cyberspace, JAPCC Journal Edition 33, 2021, p. 36–41.

This Page Intentionally Left Blank.