CYBERDEFENSE REPORT

The Law of Neutrality in Cyberspace

Sean Cordey and Kevin Kohler

Zürich, December 2021
Center for Security Studies (CSS), ETH Zürich

CSS ETH Zürich

ETH zürich

Available online at: css.ethz.ch/en/publications/risk-and-resilience-reports.html

Authors: Sean Cordey and Kevin Kohler

ETH-CSS project management: Myriam Dunn Cavelty, Deputy Head for Research and Teaching; Benjamin Scharte, Head of the Risk and Resilience Team; Andreas Wenger, Director of the CSS.

Editors: Nele Achten, Jakob Bund, and Stefan Soesanto
Layout and graphics: Miriam Dahinden-Ganzoni

DOI: 10.3929/ethz-b-000518198

Table of Contents

Glossary iv

Executive Summary 1

Introduction 3

1 Neutrality in International Relations 5
1.1 History 5
1.1.1 Origins 5
1.1.2 Codification 5
1.1.3 UN Charter and Swiss Neutrality 6
1.2 Functions 7
1.3 The Law of Neutrality 8
1.3.1 Applicability 8
1.3.2 Rights and Duties 9
1.4 Types of Neutrality 10
1.5 Neutrality Policy 10

2 Analogies 12
2.1 Background 12
2.1.1 Legal Reasoning 12
2.1.2 Relational Reasoning 12
2.2 Information- and Communication Technology 13
2.2.1 Telegraph 13
2.2.2 Telephone 15
2.2.3 Radiotelegraph 15
2.2.4 Cyberspace 17
2.3 Analysis 17
2.3.1 Structural Similarities 17
2.3.2 Structural Dissimilarities 18
2.3.3 Teleological Issues 18
2.3.4 Historical Baggage 18
2.4 Application 18

3 The Law of Neutrality in Cyberspace 22
3.1 Applicability to Cyberspace 22
3.1.1 International Law 22
3.1.2 International Humanitarian Law 23
3.1.3 Law of Neutrality 24
3.1.4 Threshold of Application 25
3.2 Neutral Duties 28
3.2.1 Peacetime Obligations 28
3.2.2 Non-participation/Abstention 29
3.2.3 Prevention 34
3.2.4 Impartiality 38
3.2.5 Acquiescence 40
3.3 Belligerent Duties 41
3.3.1 Territorial Integrity of Neutrals 41
3.3.2 Cyber Operations against a Neutral State 41
3.3.3 Cyber Operations from Neutral Territory or Infrastructure 42
3.3.4 Cyber Operations through Neutral Territory or Infrastructure 44
3.4 Remedies to Violations 45
3.4.1 General Requirements 45
3.4.2 Reparations 46
3.4.3 Retorsion 47
3.4.4 Countermeasures 48
3.4.5 Forceful or Armed Response 50

4 Challenges and Developments 53
4.1 Scope of Application 53
4.1.1 International Armed Conflict 53
4.1.2 Non-International Armed Conflict 53
4.1.3 Actors 54
4.1.4 Types of Cyber Operations 55
4.2 Territorial Sovereignty 55
4.2.1 Cross-cutting Domain 55
4.2.2 Degree of Control 56
4.2.3 Lawful Access 56
4.3 Impartiality 57
4.3.1 Technological Complexity 57
4.3.2 Private Exports to Belligerents 57
4.3.3 Private Global Governance 58
4.4 Opinio Juris and State Practice 59
4.4.1 Opinio Juris 59
4.4.2 State Practice 60
4.5 Looking Forward 61
4.5.1 International Consensus Building 61
4.5.2 Neutrality for Cyberspace 62

5 Conclusion 63

6 Annexes I
A. Convention (V) Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land I
B. Convention (XIII) Concerning the Rights and Duties of Neutral Powers in Naval War III
C. Rules in International Law Manuals on Neutrality in Cyberspace VI
D. *Opinio Juris* Quotes VII
E. *Opinio Juris* Sources XI

About the Authors XVI

Glossary

AP I	First Additional Protocol to the Geneva Conventions
CCDCOE	NATO Cooperative Cyber Defence Centre of Excellence
CERT	Computer Emergency Response Team
DoD	US Department of Defense
HC V	Hague Convention (V) Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land
HC XIII	Hague Convention (XIII) Concerning the Rights and Duties of Neutral Powers in Naval War
HPCR	Humanitarian Policy and Conflict Research (Harvard University)
IAC	International Armed Conflict
ICJ	International Court of Justice
ICT	Information and Communication Technology
IHL	International Humanitarian Law
IL	International Law
ILC ASR	International Law Commission Articles on State Responsibility
ITU	International Telecommunication Union
NIAC	Non-International Armed Conflict
OEWG	UN Open-Ended Working Group
UNGA	UN General Assembly
UN GGE	UN Group of Governmental Experts
UNSC	UN Security Council
WW1	First World War (1914-1918)
WW2	Second World War (1939-1945)

Latin Expressions

De minimis	Too small to be meaningful or taken into consideration
In abstracto	In the abstract
Jus ad bellum	The right to war
Jus angary	The right of a belligerent State to requisition neutral merchant vessels, aircraft, and other means of transport within their territorial jurisdiction
Jus in bello	Law of armed conflict / International humanitarian law
Opinio Juris	Legal opinion
Status quo ante bellum	The situation as it existed before the war
Supra	Above

Executive Summary

At first glance, the age-old law of neutrality and ever-evolving cyberspace might seem strange bedfellows. Yet, studying their intersection is pertinent. In a security environment characterized by increasing tension and geopolitical competition, studying neutrality provides an opportunity to explore a set of political-legal mechanisms and concepts, which historically have had protective and escalation mitigation functions and effects.

This report provides a historical and technological background to neutrality and a breakdown of the legal debates regarding the application of the law of neutrality in cyberspace. This includes the scope of applicability, its potential issues, and limitations. In parallel, the report takes stock of existing literature and current State views.

Historical and Legal Analogies

The law of neutrality explicitly discusses three electric information and communication technologies: telegraphy, telephony, and radiotelegraphy. These 19th-century technologies provide valuable insights for a discussion about neutrality in cyberspace.

First, there is a generally accepted ban on erecting military communication hardware on neutral territory. Second, neutral States do not have to restrict belligerents' access to telegraph and telephone lines, nor wireless telegraphy. However, they can restrict it as long as they do so impartially while enforcing this impartiality onto all relevant companies. Third, the transport of kinetic weapons across neutral territory is forbidden. The key question is to what degree the latter two points can be applied to data transported over computer networks. Specifically, some scholars argue that some cyberattacks are closer to kinetic weapons in terms of their effects than to traditional communications.

Application of the Law of Neutrality to Cyberspace

There is a broad consensus that international law applies to cyberspace. However, the application of international humanitarian law (IHL) (i.e., the body of law to which the law of neutrality belongs) is currently contested, notably by China, Russia, and Cuba. Despite this, a growing number of like-minded western States have recognized the application of IHL to cyberspace in its entirety, which *de facto* includes the law of neutrality. Discussions to clarify and operationalize the rules of IHL in cyberspace are seemingly on their way.

There is no consensus yet within the international community on how to apply the law of neutrality to cyberspace. For now, only six States have addressed the law of neutrality in their *Opinio Juris* on international cyber law: Italy, Romania, the United States of America, the Netherlands, France, and Switzerland. All have done so relatively superficially, providing limited guidance toward the operationalization of these rules. The Tallinn and Oslo Manuals both include separate chapters on the law of neutrality in cyberspace. There is no publicly known State practice regarding how these rules apply in cyberspace.

Nonetheless, application of the law of neutrality to cyberspace is justified by the 1996 *ICJ Advisory opinion on the Legality of the Threat or Use of Nuclear Weapons*, which states that the fundamental principles of neutrality largely apply irrespective of the domain.

Many questions remain as to the thresholds for the application of the law of neutrality. These are linked to broader legal discussions regarding the beginning of a conflict in cyberspace, the threshold for the *use of force* and *armed attacks*, and the intensity and duration of exchange required to trigger the law of armed conflict.

Neutral and Belligerent Duties

Based on scholarly literature and State *Opinio Juris*, this report scopes out a set of rights and duties for neutral and belligerent States. Far from clearly defined, these also come with many open questions.

Peacetime: A permanently neutral State should not engage in activities that could render impossible the fulfillment of its duties in the advent of war. This includes contracting any military alliance. This duty might raise questions about the legality and practicality of MilCERT cooperation.

Abstention/Non-participation: A neutral State should abstain from committing any acts of kinetic or cyber hostility against belligerents and providing them with military assistance, such as the provision of cyber weaponry or the recruitment of a cyber "corps of combatants." Open questions include the definition and inclusion of cyber weaponry, export controls for dual-use technologies, and military and technical intelligence.

Prevention: A neutral State should neither allow nor tolerate certain types of malicious activities on its territory and infrastructure. Contentious opinions abound regarding this duty, including the kind of knowledge required, the level of control over infrastructure, the required detection capabilities, or its extension beyond cyber operations from a neutral territory or infrastructure to those routed through them. In practice, implementing such a duty to cyber operations routing through neutral territory might be unrealistic and fraught with technical issues.

Impartiality: A neutral State should apply every restricting measure and prohibition in the context of its neutral duties and rights in a non-discriminatory manner toward all belligerents. The precise range of applications in cyberspace is ill-defined, but key foreseeable issues include access to network and cyber-infrastructure, sanctions, and digital trade.

Territorial Integrity: A belligerent State should respect a neutral State's territorial integrity. This transpires in a set of prohibitions and limitations to protect public or private cyberinfrastructures located within neutral territory or under a neutral State's control.

Cyber Operations against a Neutral State: A belligerent State should be forbidden from any hostile conduct against a neutral State's cyberinfrastructure. Open questions revolve around the types of prohibited cyber operations. For instance, do they need to amount to inconvenience, severe disruption, harm, use of force, or intrusion? What about cyber espionage?

Cyber Operations from a Neutral State: A belligerent State should be prohibited from conducting cyber operations from a neutral cyberinfrastructure. Discussions revolve around the types of prohibited cyber operations (i.e., all types of harmful activities versus acts of hostility, espionage, or force).

Cyber Operations through a Neutral State: A belligerent State should abstain from routing cyber operations through a neutral territory and cyberinfrastructure. However, routing through the Internet should be legal. This ongoing and contentious debate revolves around understanding cyber operations as weapons or communication.

Remedies to Violations: Neutral and belligerent States can willingly or unwillingly violate their duties, in which case the injured State has a right to remedies. Depending on the violations, these include reparations, retorsion, countermeasures, and, in some instances, forceful responses. Each remedy has its own set of requirements.

Discussion: Relevance, Limits, and Opportunities

The extent to which the law of neutrality will further develop remains uncertain. Currently, there are political disincentives and legal and practical challenges for its development and relevance for cyberspace.

The main limitation is its scope of applicability, which is limited to international armed conflicts (IAC) and State actors. Most confrontations in cyberspace occur below the threshold of an IAC, and involve a diverse set of actors, including private and non-state actors. Furthermore, the challenge of attribution and the often-ambiguous nature of cyber operations, most of which can be defined as espionage, also make applying the law of neutrality difficult.

An additional challenge is that cyberspace is an artificial environment spanning all other operational domains, each comes with different conceptions of sovereignty and legal frameworks. For instance, the neutral prevention duty is absolute on land but relative on the seas. The traditional attachment of the law of neutrality to territorial sovereignty also poses practical challenges for States, notably regarding the expected degree of control and access to outgoing and transiting data from ones' territory.

The interconnected, privatized, and decentralized nature of cyberspace, its infrastructure, and governance also make the applying the central tenets of neutrality arduous, particularly the impartiality duty and the development of a credible neutral posture.

Politically speaking, the law of neutrality in cyberspace remains a niche that is often misunderstood and rarely ranks high among States' priorities. Some States may even fear the additional burden or operational limitations the law of neutrality could entail if further developed.

Permanent neutrality, however, is not limited to its legal component. It also entails a political factor. States may thus consider potential avenues and issues for their neutrality policy in cyberspace. Among other things, it could be helpful to think back to the solidarity function of neutrality. This could take the form of preventive diplomacy, good offices, capacity building, or mediation.

Conclusion

Debates about the application of the law of neutrality in cyberspace are still in their infancy. While we can highlight a set of potential rules, their development and operationalization remain uncertain in the short- and long-term due to their legal and political limitations as well as the uneasy balance of interests between belligerent and neutral States. To be useful and actionable, they require more in-depth discussion, State *Opinio Juris*, and State practice. Such discussions require expertise and attention, particularly from neutral parties.

Finally, neutrality is neither an end in itself nor a fixed and rigid legal concept or policy instrument. Both neutrality policy and law have evolved historically, including in response to technological innovations and shifts in geopolitics. They have the capacity for further development and adaptation to cyberspace's specificities and realities.

Introduction

The law of neutrality and cyberspace are seemingly strange bedfellows. Neutrality is a legal and political concept that gradually emerged within the European balance of power system. Its primary legal documents are the 1907 Hague conventions, designed to deal with conflicts between sovereign States above the threshold of war. The international legal sources have not changed substantially since. In contrast, neutrality policy has been an adaptive foreign policy tool. As stated by the Swiss Federal Council in its 1993 report on neutrality, "neutrality has never been a rigid institute, but a flexible instrument for safeguarding interests. The meaning and content of neutrality have always depended on the foreign and security policy environment."[1]

In contrast to neutrality's legal and policy underpinnings, cyberspace is a forward-looking concept that first emerged in science-fiction in 1984. It became a recognized and dedicated domain for human interaction and conflict in the 1990s. Having grown rapidly alongside the global Internet, it now permeates most modern societies and lives, providing both opportunities and threats. Malicious cyber operations, for instance, have become a persistent peacetime and wartime phenomenon. While States sponsor some cyber operations, non-state actors are seemingly predominant in this space. States and the international community still struggle to agree on shared norms and rules.

Despite the seemingly irreconcilable spirit of the two concepts, exploring, discussing, and analyzing their intersection seems relevant for the reasons outlined as follows.

<u>The Value of International Law in a Context of Instability</u>

The current international security environment is characterized by increasing strategic competition between great (cyber) powers. Furthermore, both the societal dependency on digital infrastructure and the impact of cyber operations continue to grow every year. **Hence**, **it is pertinent to explore political-legal mechanisms and concepts, which historically had protective and escalation mitigation functions**.

Despite the practical and historical realities, international law remains fundamental to the stability and predictability of inter-State relations, at least within the current rules-based liberal order. As reemphasized by the UN GGE reports, international law is also the basis for States' shared commitment to preventing conflict and maintaining international peace and security, and it is key to enhancing confidence among States. Meanwhile, international humanitarian law (IHL) and the law of neutrality also remain vital instruments to reduce risks and potential harm to civilians, neutrals, infrastructure, and combatants in the context of armed conflict.

Despite encouraging progress over the past years, notably at the UN level, there is still no global consensus as to how to apply international law, including the law of neutrality, to cyberspace. **In preparation for necessary discussions about clarity and concrete applicability, it is helpful for legal experts and policymakers to have an overview of ongoing discussions, potential issues, and pitfalls**.

<u>Context-dependent Development of the Law of Neutrality</u>

Discussions about neutrality in cyberspace are still in their infancy. The development of this body of law and related policies will depend, in part, on the interpretations of interested States. A formal amendment to the 1907 Hague rules to include cyberspace is unlikely to happen soon. However, States will probably continue to attempt to apply and interpret provisions of neutrality law as they see fit, depending on current geopolitical interests and technological conditions. The recently published opinions on international cyber law by France, the Netherlands, Italy, Romania, and Switzerland indicate such a trend.

The uneasy balancing of interests between belligerents and neutral States will inevitably evolve. As it has historically been the case, one can expect great powers to have some leverage to either further develop or undermine this body of law. However, the technological capabilities of neutral States and their economic and political interests will also play a role in this balancing.

To anticipate the potential direction of the law of neutrality in cyberspace and the potential burdens attached to it, it is insightful to have an overview that situates the current debate, the stakes, and various State positions.

<u>Potential Interest of Neutral States</u>

All States that rely on a rules-based system have an interest in predictable behavior in cyberspace. This includes behavioral expectations regarding what constitutes neutral behavior and what constitutes non-neutral behavior. **Permanently neutral States, which rely on their reputation as neutrals and have peacetime obligations, have a specific interest in closely following – if not directly participating in and shaping – the development and application of IHL and the law of neutrality to cyberspace.**

This interest needs to be balanced against the political and strategic realities of international affairs. Indeed, in the current state of application of IHL and discussions of cyber neutrality, neutral States, and most

[1] Schweizerischer Bundesrat. (1993). Bericht zur Neutralität: Anhang zum Bericht über die Aussenpolitik der Schweiz in den 90er Jahren vom 29. November 1993. p.3.

other States, have a strong disincentive to further develop their obligations without additional and more precise commitments in return.

This may change in the future as security stakes rise and specific cases or cyber-enabled conflicts arise. The fact that China and the US are already exerting diplomatic pressure on smaller States over public statements and technology procurement to push them to choose sides might renew the interest in – and the potential relevance of – the law of neutrality and neutrality policy more broadly.

Lastly, in permanent neutral States like Switzerland, neutrality continues to be an essential part of the national ethos and an instrument in its foreign and security policy. Neutrality is a sensitive, emotional, and complex subject. Hence, it regularly re-emerges in public, policy, political, and legal debates. This is also true for cyber neutrality, which has raised some interest in Switzerland. There have notably been panels on neutrality and cyberspace at the Swiss and international Internet Governance Forum and Geneva Peace Week, a parliamentary intervention by Damian Müller[2], and articles and a white paper by former Ambassador Dahinden, Sara Pangrazzi, and ICT4Peace.[3]

Aim and Outline

This report does not prescribe a specific operationalization of neutrality. Instead, it aims to provide a broad historical, technological, and legal background in addition to an in-depth breakdown of the international legal debates over the law of neutrality in cyberspace. This includes the scope of applicability, its potential issues, and its limitations. In parallel, this report aims to take stock of existing literature and, more importantly, current State views on the matter. The report is structured as follows:

Section 1 provides historical and legal background on the origin, types, and concepts of neutrality and the law of neutrality. Section 2 explores and maps out the communication technologies the law of neutrality explicitly refers to and to what degree these can be analogized to computer networks. The background information provided in Sections 1 and 2 is primarily geared toward researchers. **Readers interested in discussions about the concrete application of neutral rights and duties may skip directly to Section 3,** which provides an overview of how States and legal scholars interpret the application of the law of neutrality to cyberspace. Section 4 analyzes these discussions and highlights, amongst other things, the limitations and challenges of the law of neutrality applied to cyberspace. Section 5 concludes the report.

Please note the following disclaimer: This report is based exclusively on publicly accessible sources, ranging from academic literature, State *Opinio Juris*, and State practice, some of which were derived from archival work conducted by the authors.

[2] Müller, D. (2021) La Suisse est-elle préparée à une cyberguerre du point de vue de la neutralité?.

[3] Dahinden, M. (2021). Schweizer Neutralität im Zeitalter der Cyberkregsführung. ICT4Peace.

1 Neutrality in International Relations

Neutrality is a complex and, at times, emotional topic. It possesses numerous facets: legal, political, historical, economic, and cultural. It is also a concept that most people understand and conceptualize differently, notably what it means in practice.

Hence, before any discussions on the application of neutrality to cyberspace, it seems relevant to provide a short overview of neutrality, where it originates, and what it entails. The rest of the report emphasizes the legal dimension of neutrality (i.e., the law of neutrality) which forms the core and baseline of what neutrality has been in international relations.

1.1 History

1.1.1 Origins

The status and issues of war and peace, including neutrality, are amongst the oldest aspects of public international law. The (legal) practice of neutrality can be observed as early as the 14th century.[4] However, it was mainly during the Age of Exploration (15th – 17th centuries), the subsequent rise of the nation-state, and the creation of the Westphalian system (after 1648) that the concept of neutrality gained importance and substance. The philosopher and diplomat Hugo Grotius provided the first definition of non-participation in war, arguing that "from those who are at peace nothing should be taken except in case of extreme necessity, and subject to the restoration of its value."[5]

Neutrality's development was rooted in a convergence of interests. On the one hand, the expanding European empires relied on undisrupted globalized maritime commerce. As non-belligerents, these empires had a stake in ensuring the security of their merchant fleets. Meanwhile, belligerent States were interested in enforcing the rules of maritime neutrality to their advantage and their enemies' detriment. On the other hand, smaller nations saw the economic opportunity offered by enhanced trade of wartime commodities with these belligerents.

The development and intensification of land warfare in Europe during the 17th and 18th centuries were also pivotal for the development of neutrality and the slow expansion of the rules attached to it. The Thirty Years' War and the post-Westphalia nation-state paradigm that emerged in its wake were particularly key. They fostered the concept upon which the law of neutrality, and international law more generally, rests: territorial sovereignty. Ever since, all States guard their territorial sovereignty against infringements by other States.[6] Typical territorial sovereignty and neutrality violations included boarding or capturing an enemy ship at anchor in a neutral port by a belligerent or trespassing a neutral land territory to attack.

Two important legal milestones paved the way for the emergence and the codification of the law of neutrality. The first was the *1856 Paris Declaration Respecting Maritime Law,*[7] which attempted to abolish privateering while regulating the relationship between neutrals and belligerents on the high seas. The second was the *1872 Washington Rules of Neutral Duty*,[8] which imposed upon the neutral party a duty of due diligence in protecting foreign merchants.[9]

These early international rules of neutrality stem from a period characterized mainly by concerns over economic warfare and assertion of the principle of *freedom of the seas*. Further important factors and events in neutrality's development were:

1. The two Leagues of Armed Neutrality of 1780 and 1800. These alliances of European naval powers aimed to protect neutral shipping against the UK's policy of unlimited search of neutral shipping for French contraband.
2. The standing neutrality policy of the United States of America, which was enshrined by George Washington and initially maintained in both World Wars.
3. The acceptance by the international community of Switzerland (1815) and Belgium (1839) as the first permanently neutral States.[10]

1.1.2 Codification

Having gradually become part of customary international law, neutrality was further codified at the Second Hague Peace Conference, organized at the suggestion of US President Theodore Roosevelt. Following it, **the main sources of the law of neutrality became, and still are, the 1907 *Hague Conventions V* and *XIII* (HC V and HC XIII)**. The former relates to the

[4] Higson, D. (2016) "Applying the Law of Neutrality While Transitioning the Seas of Cyberspace," *American University National Security Law Brief*, 6(2); see Jessup, P. & Deak, F. (1976). Neutrality: its history, economics and law. Columbia University Press.

[5] Grotius, H (1646/1925), De Jure Belli ac Pacis [On the laws of war and peace], 2:3, London: Humphrey Milford.

[6] Turns, D. (2015). *Cyber war and the law of neutrality*, in Research Handbook on International Law and Cyberspace, chapter 18, pp. 380-400.

[7] The declaration is the outcome of a *modus vivendi* signed between France and Britain in 1854, originally intended for the Crimean War (1853-1856). These two powers had agreed that they would not seize enemy goods on neutral vessels nor neutral goods on enemy vessels.

[8] Verzijl (1979). International Law in Historical Perspective: The Law of Neutrality.

[9] Gavouneli, M. (2012). "Neutrality – A Survivor?", *The European Journal of International Law*, 23 (1), pp. 267-273.

[10] Schindler, D., & Toman, J. (1988). "The Laws of Armed Conflicts", Martinus Nijhoff Publisher.

rights and duties of neutral powers and persons in land warfare, while the latter relates to naval warfare.

In addition to these two 1907 Conventions, several other Hague Conventions adopted in 1907 encompass specific provisions relevant for neutrality. These are: *Convention VIII relative to the Laying of Automatic Submarine Contact Mines*; *Convention XI relative to Certain Restrictions with Regard to the Exercise of the Right of Capture in Naval War*; *Convention VII relative to the Conversion of Merchant Ships into War-Ships*; and *Convention XII relative to the Creation of an International Prize Court*.

The codification efforts stopped with the advent of the First World War, where many of these rules were put to the test – often failing. It was not before 1923 that the efforts began anew with the drafting of the Hague Conventions on aerial warfare and wireless telegraphy. However, these *Rules for the control of wireless telegraphy in time of war* and *Rules for Air Warfare* were never converted into a treaty.

The law of neutrality continued to develop post-1907, albeit in a limited fashion.[11] Rules concerning neutrality in the three traditional domains of war (land, sea, air) were restated and further developed in various international legal documents of which only some are treaties, such as the unratified 1909 *Declaration of London,*[12] the 1928 *Havana Conventions*,[13] the *1938 Stockholm declaration*, the 1949 *Geneva Conventions and its* 1977 *Protocol I*, or the 1998 *Helsinki Principles.*[14]

1.1.3 UN Charter and Swiss Neutrality

Neutrality rules were adopted when international law allowed sovereign States to resort to war to resolve disputes. This changed with the 1919 *Covenant of the League of Nations* and the 1928 *Separate General Treaty for Renunciation of War as an Instrument of National Policy* (a.k.a. the *Kellogg-Briand Pact*).

Switzerland was able to find an agreement with the League of Nations, which recognized its neutrality and excluded it from taking part in military sanctions. In exchange, Switzerland switched from a policy of *integral neutrality* to one of *differential neutrality* in which it would support League decreed economic sanctions. However, Switzerland was unwilling to support the economic sanctions imposed by the League against its southern neighbor Italy for its invasion of Ethiopia and returned to an *integral neutrality* policy in 1938.

With the end of the Second World War and the adoption of the United Nations Charter (UNC) in 1945, the UN collective security system essentially outlawed the use of force under Article 2(4) UNC and required the cooperation of all member States with collective security enforcement action mandated by the Security Council under Chapter VII and Article 2(5). As a result, it was envisioned that a neutral State could not uphold its impartiality duty towards belligerents once the UN Security Council (UNSC) has ordered enforcement measures.[15]

Despite this potential incompatibility, several permanent neutrals (e.g., Sweden and Austria) subordinated their neutrality to UN law, but not Switzerland. Indeed, it was this perception of incompatibility between UN law and its neutrality, the US's critical view of Switzerland's opportunistic neutrality during WW2, and the UN's strict refusal to grant an exception, amongst other things,[16] that drove Switzerland not to join the UN when it was set up.

During the Cold War, Switzerland officially enforced a policy of *integral neutrality* based on the very strict *Bindschedler Doctrine*. The latter entailed that to remain credible as neutral, Switzerland should adopt and implement a dogmatic abstentionist conception of neutrality: no collective security organization, no military alliances, no economic sanctions, no customs unions. This policy was also partly driven by economic interests as it guaranteed continuous commerce.

In practice, however, Switzerland was more integrated into the Western bloc and was anti-communist, banning the communist party as early as 1943. The doctrine also didn't hold against the intense diplomatic pressure from the US. In 1951 the Swiss government secretly adopted controls over the export of strategic goods to the Soviet bloc similar to those adopted by the member states of the Coordinating Committee for Multilateral Export Controls (COCOM).

The *Helsinki Final Act* in 1975 was a decisive step toward the recognizing neutrality following the establishment of the UN. It also indicated a change in the view of the US, which had been critical of neutrality since WW2. As such, the accord clearly stated that "within the framework of international law, all the participating States have equal rights and duties. [...] they also have the right to neutrality."[17] In addition to the explicit recognition of neutrality, neutral States (i.e., Sweden, Switzerland, Finland, and Austria) played a key role during the negotiations. Unable to influence the

[11] Boothby, W., & Heintschel Von Heinegg, W., (2018). The Law of War: A Detailed Assessment of the US Department of Defense Law of War Manual. Cambridge University Press.
[12] The Declaration of London (1909).
[13] Convention on Maritime Neutrality, Havana (1928).
[14] International Law Association (1998). *Helsinki Principles on the Law of Maritime Neutrality, Final Report of the Committee on Maritime Neutrality, International Law Association, Report of the 68th Conference*, Taipei.
[15] Turns, *supra* note 6.
[16] For an interesting read of Swiss Neutrality Policy in the Cold War, see Fischer, T. & Möckli, D. (2016). "The Limits of Compensation", *Journal of Cold War Studies* Vol. 18, No. 4, Fall 2016, pp. 12–35; Wenger, A. & Nuenlist, C. (2008). "A 'Special Case' between Independence and Interdependence: Cold War Studies and Cold War Politics in Post–Cold War Switzerland," *Cold War History*, Vol. 8, No. 2. pp. 213–240.
[17] The Helsinki Final Act (1975).

first and second baskets of the accord, which dealt with major security and political issues, they seized the pivotal third basket on human rights as their opportunity to influence the course of the negotiations.[18]

Following the end of the Cold War, the strict conception and policy of Swiss neutrality slowly changed. Neutrality was finally deemed compatible with the UN regime, culminating in Switzerland's accession in 2002 and shift toward a more cooperative neutrality policy: *active neutrality*.

Overall, despite continued enforcement of some neutrality policies by permanent neutrals, there was a general tendency to dismiss the law of neutrality as obsolete following the UN's establishment and the institution of UN law. Such a position was inopportune, if not inadequate, for several reasons.

Firstly, many scholars, such as *Drew*, vigorously dispute its obsolescence. [19] Some notably find solace in the separate opinion of Ammoun in the 1971 ICJ *Namibia Advisory Opinion* of the International Court of Justice, which has a clear judicial assertion that the law of neutrality continues to be in force: *"If the provisions of the Charter concerning collective security could have been implemented according to the letter and in the spirit of the San Francisco Conference, there would have been no place for neutrality, at least among States Members of the United Nations. (…) The Security Council's action has been paralyzed by the veto, or by the fear of a veto (…) Consequently, neutrality persists so long as wars are tolerated, whether deliberately or through weakness."*[20] But many point toward the ICJ's 1996 *Nuclear weapons* advisory opinion, which reaffirmed the continued survival of neutrality as "an established part of the customary international law."[21]

Secondly, the terms *neutral* and *non-belligerent*[22] have been regularly used in recent codification attempts and treaties, notably in the *Geneva Conventions*. Similarly, several legal expert manuals have restated or modernized the language of the rules: e.g., the 1994 *San Remo Manual on International Law Applicable to Armed Conflicts at Sea*, the 2009 *HPCR Manual on International Law Applicable to Air and Missile Warfare*, the 2013/2017 *Tallinn Manual on the International Law Applicable to Cyber Operations*, and the 2020 *Oslo Manual on Selected Topics of the Law of Armed Conflicts.*[23] The last two contain explicit rules for applying the law of neutrality in cyberspace (see Annex C). Some neutrality rules have also been restated in military manuals and national judicial decisions (e.g., in the US, the UK, Canada, Germany, Denmark, and the Netherlands).[24]

Thirdly, the laws of neutrality have also been complemented by evolving State practices. *Heintschel von Heinegg*[25] points to the fact that post-WWII, State practice shows that the law of neutrality has been applied in every international armed conflict (IAC), irrespective of whether neutral States wished to be bound by it or not. However, in many of these conflicts,[26] the rules laid down in HC V and XIII were not always strictly adhered to. Thus, according to modern State practice, the applicability of the law of neutrality depends on functional considerations that often result in a differential or partial applicability of that body of law.

Hence, it is safe to say that the law of neutrality has not only survived but has been enriched by some codification efforts, the accumulation of State practices and *Opinio Juris*, and the growth of jurisprudence.[27]

1.2 Functions

Neutrality has historically had intertwined and mutually-reinforcing legal and political functions.

The primary legal function of the law of neutrality is to regulate the relationship and co-existence between the belligerents in an international armed conflict and States that are not party to the conflict **to prevent the escalation of the conflict**.[28] In other words, the law of neutrality provides the conditions upon which neutral States may continue to

[18] Molineu, H. (1978). "Negotiating Human Rights: The Helsinki Agreement." *World Affairs,* 141(1), p. 26.

[19] Drew, P. (2017). "The Law of Maritime Blockade: Past, Present, and Future", Oxford University Press.

[20] Ammoun, F. (1971). Legal Consequences for States of the Continued Presence of South Africa in Namibia (South West Africa) notwithstanding Security Council Resolution 276 (1970): Separate Opinion of Vice-President Ammoun. p. 8.

[21] ICJ (1996). Legality of the Threat or Use of Nuclear Weapons.

[22] As highlighted by Boothby & Heintschel von Heinegg, that term was used as a compromise formulation because the delegates negotiating the Geneva conventions were unwilling to provide statements as to the continuing validity of the law of neutrality.

[23] This latest attempt builds on the previous HPCR and San Remo manuals and goes beyond missile and air warfare, including dedicated sections on outer space and cyber operations.

[24] E.g. the 1992 German Joint Services Regulations (ZDv15/2); UK Ministry of Defence, *The Manual of the Law of Armed Conflict* (OUP 2004); US Department of the Navy *et al.*, *The Commander's Handbook on the Law of Naval Operations*, NWP 1–14M (ed July 2007); US DoD *Law of War Manual* (2015). *Canadian Manual* Law of Armed Conflict at the Operational and Tactical Levels, ch. 13; The Federal Ministry of Defence of the Federal Republic of Germany, Humanitarian Law in Armed Conflicts – Manual, Chapter 11 (Bonn 1992).

[25] Heintschel von Heinegg, W. (2007). *Benevolent Third States in International Armed Conflicts: the Myth of the Irrelevance of the Law of Neutrality* in International Law and Armed Conflict: Exploring the Faultlines.

[26] For instance, the Falkland/Malvinas conflict or the Iran-Iraq war.

[27] See section 1.2.2 for a detailed list of modern reiteration of the law of neutrality. Otherwise see Schindler, D. (1991). "Transformations in the Law of Neutrality since 1945", in: Humanitarian Law of Armed Conflict – Challenges Ahead, Essays in Honour of Frits Kalshoven, 367-386 (ed. by A.I.M. Delissen/G.J. Tanja, Dordrecht); Heintschel von Heinegg, W. (2004). "Wider die Mär vom Tode des Neutralitätsrechts", in Crisis Management and Humanitarian Protection, Festschrift für Dieter Fleck, 221- 241 (ed. by H. Fischer et al., Berlin).

[28] Bothe, M. (1999). *The Law of Neutrality,* in The Handbook Of International Humanitarian Law. p. 549.

maintain peaceful relations with belligerents while preventing belligerents from interfering with the sovereignty of neutral States.

The broader political-legal functions of neutrality are intended: to protect neutral States' territorial sovereignty and their citizens against the conflict's harmful effects; safeguard neutral rights, such as engaging in commerce; and protect parties to the conflict against interferences.[29] According to the Swiss scholar *Riklin,*[30] neutrality has five political functions listed in Table 1.

Independence	To maintain foreign and security policy autonomy while limiting the harmful effects by staying away from the conflict.
Free Trade	To ensure continuous access to commerce despite a conflict.
Balance of Power	To contribute to the stabilization of the European continent during the 19th and 20th centuries by fixing (geographical) components of the theater of war (e.g., Alpine pass or acting as buffer State).
Integration	To help harmonize diverse (e.g., cultural or religious) stakeholders during conflicts by promoting a shared foundational myth/ideal/ ambition.
Solidarity	To help mediate and prevent international conflicts, notably through good offices, while also providing a continuous justification to the international community for upholding neutrality.

Table 1. The five political functions of neutrality, according to Riklin (1991)

1.3 The Law of Neutrality

1.3.1 Applicability

The law of neutrality refers to a body of rules and principles that regulate the rights and duties of belligerent and neutral States during armed conflicts between sovereign States. The legal application of neutrality is thus tied to issues of definition and recognition of IACs. This includes questions of threshold (e.g., for an *armed attack*) or conflict duration and intensity – all of which echo in cyberspace (Section 3.1). The legal rules applicable during armed conflicts are referred to as *jus in bello, International Humanitarian Law* (IHL), or the *Law of Armed Conflicts*.[31] As pointed out by *Heintschel von Heinegg,*[32] international lawyers, legal scholars,[33] and States continue to almost unanimously maintain that the existence of a state of war automatically triggers the applicability of the law of neutrality. Some, like France, traditionally require a declaration of war. Meanwhile, Sweden claims that its applicability depends on a formal declaration by a neutral State. Still, others, like the US, believe that the law of neutrality is applicable in every IAC when intense hostilities of a certain duration characterize the conflict.[34]

While the rules applicable during IACs generally do not require a minimum threshold of intensity of the international armed conflict, some scholars have suggested that there should be a minimum threshold for the law of neutrality to apply. *Roscini* and *Bothe*[35] argue that because the application of neutrality rules considerably modifies the parties' relationships while limiting their rights, it can only be justified when the conflict is serious enough and when the law of neutrality becomes meaningful and necessary.

The US's *Law of War Manual* also adopts this view, stating that "the duties of neutral States to refrain from certain types of support to belligerent States do not apply to all armed conflicts to which *jus in bello* rules apply such duties are only triggered in armed conflicts of a certain duration and intensity."[36]

[29] Heintschel Von Heinegg, W. (2012). *Neutrality in Cyberspace*, 4th International Conference on Cyber Conflict. Tallinn.

[30] Riklin, A. (1991). "Fonctions de la neutralité suisse", *Passé pluriel*. En hommage au professeur Roland Ruffieux, Fribourg, Éditions universitaires, 1991, pages. 361-394.

[31] Currently, the Law of neutrality applies to NIAC only through an exception: where the insurgents have been recognized as belligerents or the conflict is a war of national liberation according to Article 1(4) of Protocol I additional to the 1949 Geneva Conventions on the Protection of Victims of War. In traditional non-international armed conflicts (NIAC), third states are generally precluded from intervening in any form on the side of the insurgents under the customary principle of non-intervention.

[32] Heintschel von Heinegg, *supra* note 25.

[33] *See* e.g., *Kotzsch*, L. (1956). "The Concept of War in Contemporary History and International Law", at 141; *Schindler*, D. (1979). "State of War, Belligerency, Armed Conflict", in: The New Humanitarian Law of Armed Conflict, 3-20, at 5 et seq. (ed. by A. Cassese, Napoli); *Greenwood*, C. (1987). "The Concept of War in Modern International Law", 36 *International and Comparative Law Quaterly* 283-306, 305 (1987); *Rousseau*, C. (1983). "Le droit des conflits armés", at 371.

[34] Boothby & Heintschel von Heinegg, *supra* note 11. "The divergence of positions may be explained by the fact that during the (few) international armed conflicts of recent decades, the aggrieved belligerents were simply unable militarily or otherwise to respond to, or terminate, violations of the law of neutrality."

[35] Roscini, M. (2014). *Cyber operations and the Law of Neutrality*, in Cyber operations and the use of force in international Law, Oxford publishing; Bothe, *supra* note 28.

[36] US DoD, *supra* note 24, para 15.2.1.2.

However, as a commentary by *Boothby* and *Heintschel von Heinegg* justly points out, there remains an "obligation of belligerents to respect the sovereignty of neutral States in all international armed conflicts, thus recognis[ing] that the essential rules of the law of neutrality will apply irrespective of the duration and intensity of an international armed conflict. The importance of that recognition, which is also shared by the ICJ's Nuclear case. The San Remo Manual and the AMW Manual, must not be underestimated."[37]

While the application of the law of neutrality depends on the recognition of an IAC, two (or more) States may conduct hostilities against each other but refuse to recognize a state of armed conflict. In that case, some scholars, such as *Tucker,*[38] posit that third States may reject this position and invoke the law of neutrality to protect their rights in relation to the armed conflict. The US takes that position too.

The law of neutrality traditionally ceases to apply when the conflict in question ends, which usually entails a certain degree of normalization of relations and lack of hostilities. Alternatively, the law of neutrality will stop regulating the relationship between neutral and belligerent States as soon as the neutral State loses or ends its neutral status.

To sum up, while State practice tends to prove the continuing validity of the law of neutrality to this date, there is a consensus that the law of neutrality applies during IAC or state of war. There are, however, some differing views as to when precisely that body of law starts applying once an international armed conflict has arisen.

1.3.2 Rights and Duties

The law of neutrality entails specific rights and duties underpinning the relationship between neutral and belligerent States. They can be understood as both correlative and reciprocal, meaning that the duties of neutrals often correspond to the rights of belligerents and vice-versa. Similarly, the ability and authority of a neutral State to assert its rights may depend on whether it has fulfilled its corresponding neutral duties.

The key principles and obligations of neutral States can be summarized as follows: *Non-participation/Abstention*, *Prevention*, *Impartiality*, and *Acquiescence* (see Table 2).

The underlying principle of the law of neutrality is that the territorial sovereignty of a neutral must not be violated (by a belligerent) – or as Article 1 HC V puts it: *"The territory of neutral Powers is inviolable."* This principle is reiterated in Article 2 HC XIII. Territorial inviolability, however, differs between military domains. While it is absolute on land, it is relative at sea. For instance, the presence of a belligerent warship in neutral territorial waters can be legal if it abstains from conducting any hostilities (Article 1 and 2 HC XIII) – i.e., the customary right of innocent or peaceful passage. Air operations are also differentiated between whether they take place over land or sea.[39]

Apart from respecting neutral commerce, **belligerents have to respect the territorial inviolability of a neutral State**: by abstaining from certain hostile conduct, including moving troops, weapons, and other materials of war across neutral territory (Article 2 HC V; Article 5 and 8 HC XIII), air or waters; erecting and using wireless telegraphy to communicate for military purposes (Article 3 HC V); and recruiting "combatant corps" on the neutral State's territory (Article 4 HC V).

In return, the neutral State has several negative duties. The first is to abstain from committing any hostile acts against the belligerents, providing them with military assistance, or allowing the use of their territory for the conduct of hostilities (Article 2 and 3 HC V; Article 6 HC XIII). Again, the exact rules vary depending on the domain. For instance, the scope of the latter obligation extends to support activities carried out by their subjects within their territory but excludes belligerent merchant vessels that are not operating under the direction or control of a belligerent for hostile or military purposes.[40] An important caveat is that the neutral State is under no obligation to prevent its citizens from assisting any belligerent party when their actions are conducted outside of the neutral State's territory. However, the involved citizens might lose their status as neutral persons and their legal protections in such situations (Article 6 and 17 HC V; Article 7 HC XIII).

The neutral State **has the positive duty to exercise its best efforts to terminate and prevent any violations of its neutrality**, including by using force, if necessary (Article 5 HC V; Article 25 HC XIII).[41] During WWI and WWII, for example, Switzerland diplomatically protested and militarily engaged hundreds of belligerent aircraft that mistakenly or purposefully violated Swiss airspace. Importantly, this duty is one of conduct, meaning that a neutral State has an obligation of best efforts. An important exemption to this duty concerns the use of telegraphic, radio, or telephonic communication infrastructure (Article 8 HC V).[42]

Another positive duty for neutrals is impartiality and non-discrimination. The neutral State must apply every measure of restriction and prohibition

[37] Boothby & Heintschel von Heinegg, *supra* note 11

[38] Tucker, R. (1955). *The Law Of War And Neutrality At Sea*, Washington: United States Government Printing Office, pp. 199-200

[39] See HPCR rules 167(a), 172(a) and 172(a)(ii).

[40] Nasu, H. (2020). *The Laws of Neutrality in the Interconnected World: Mapping the Future Scenarios,* in The Future of Law of Armed Conflict. Oxford University Press.

[41] Resort to force by a neutral nation to prevent violation of its territory by a belligerent does not constitute an act of hostility. Cf. Article 10 HC V.

[42] Although Hague XIII, Article 5, addresses the erection of communication apparatus, during World War II, practically all neutral nations prohibited the employment by belligerents of radiotelegraph and radiotelephone apparatus within their territorial sea.

in exercising their rights and duties with complete impartiality towards all the belligerents. This duty is subjective, which means that it does not require restrictive measures to have an equal effect upon all belligerent States, nor do they have to be intended as such.[43] Some specific restrictions and prohibitions, such as those involving trade, are not considered hostile acts. Interestingly, no prohibitions on exportation and transportation exist "on behalf of one or other of the belligerents, of arms, munitions of war, or, in general, of anything which can be of use to an army or a fleet" (Article 7 HC V). In such cases, the duty of non-discrimination does not mean that sales must be extended equally to both sides in a conflict, although if a neutral State decides to ban such exports, it must do so on a non-discriminatory basis (Article 9 HC V). The principle of impartiality should apply to "the admission into its ports, roadsteads, or territorial waters, of belligerent war-ships or of their prizes" in a conflict at sea (Article 9 HC XIII).

Lastly, suppose a neutral State is unwilling or unable to prevent the use of its territory for hostile operations against a belligerent (a failure which comes within the definition of aggression in customary IL and a violation of its neutral duties).[44] In that case, the latter may be entitled to use certain remedies in self-defense/help against hostile forces in the neutral State. Accordingly, **the neutral State must acquiesce the belligerent's exercise of his remedies** against him (and its subjects) if it violates its duties under the law of neutrality (e.g., by engaging in hostile assistance or failing its prevention duty).

	Neutrals	Belligerents
Rights	• Inviolability of its territory • Neutral commerce	• Insist on neutral's duties • Self-help in case of violation
Duties	• Abstention • Prevention • Impartiality • Acquiescence	• Respect the neutral's inviolability and commerce

Table 2: Reciprocal rights and duties

1.4 Types of Neutrality

The law of neutrality under the Hague Conventions applies to all States that remain neutral in a conflict. Nevertheless, **it is important to differentiate between *temporary neutrality* and *permanent neutrality*. The former,[45] also known as *conflict neutrality,* is limited to a specific international armed conflict and may even change during that conflict**.[46] For instance, while Belgium had a position and status of neutrality at the outset of WWII, it became a belligerent when Germany invaded it. Vice versa, a belligerent State can withdraw from a conflict and become neutral vis-à-vis the remaining belligerents, as was Russia's case following the Brest-Litovsk treaty in WWI.

Temporary neutrality is not to be confused with *non-belligerency*, which is the practice certain States (e.g., Italy from September 1939 to June 1940) adopted to allow for assistance to a belligerent without direct involvement in armed hostilities.[47] Such a policy violates the neutral duties of abstention and impartiality. Confusingly, it is also sometimes referred to as *benevolent neutrality.*

Permanent neutrality, meanwhile, is not affected by the temporal existence of any particular armed conflict and is a matter of legal obligations even in peacetime, be it voluntary as a matter of domestic law (e.g., Switzerland)[48] or imposed by an international treaty (e.g., Austria).[49] Permanent neutrality entails duties that apply before the commencement of and independently from an IAC. In particular, **a permanently neutral State is obliged not to abstain from hostilities when an armed conflict breaks out but also to refuse any military obligations and abstain from acts that would render the fulfillment of its neutrality obligations impossible should the international armed conflict occur**. This would include, for instance, becoming a member of a military alliance.

Permanent neutrality is not to be confused with *de facto neutrality*, which may occur when a State has abolished its armed forces; Liechtenstein and Costa Rica are two examples of this phenomenon.

Furthermore, a designated part of a State's territory can also be permanently neutral. For instance, the Panama Canal Zone was declared neutral in perpetuity under Article XVIII of the 1903 *Hay-Bunau-Varilla Treaty* and reconfirmed under Article 1 and 2 of the 1977 *Torrijos-Carter Treaties*.

1.5 Neutrality Policy

Aside from the legal distinction between *permanent neutrality* and *conflict/temporary neutrality,* a further distinction must be made between the narrow legal

[43] Nasu, *supra* note 40.
[44] UNGA Res 3314 (XXIX).
[45] i.e. the de jure status of non-participating States of a specific conflict.
[46] Turns, *supra* note 6.
[47] Ibid.
[48] i.e. the Swiss Constitution provides that the Federal Council and the Federal Assembly must take measures to safeguard Switzerland's neutrality. Neutrality, however, is not designated as a purpose of the Federation or as a foreign policy principle. Switzerland, however, highlights in numerous reports that it is at liberty to give up its neutrality unilaterally without violating international law.
[49] Further examples include Belgium following the 1839 treaty of London or the Vatican City State under art 24 of the Treaty of Conciliation, part of the 1929 Lateran Pacts with Italy, as a condition of continued papal independence following Italian unification.

obligations that arise from the law of neutrality and the broader neutrality policies that countries adopt and enact. A neutrality policy refers to the steps that a neutral country takes to preserve its neutrality. These often go beyond domestic or international legal obligations and their common interpretations. It is a unilateral policy decision that can be modified or reversed and, as such, does not require international recognition. In many respects, the *Hague Conventions* set a minimum bar for the strictness of neutral duties, but States are free to take more comprehensive measures to maintain a neutral status.

Table 3 below provides some common examples of named neutrality policies. Some have specific characteristics or apply in specific cases, such as *qualified neutrality*, while others are more all-encompassing, such as *armed neutrality*. *Differential* and *integral neutrality* are, however, mutually exclusive. *Active* and *armed neutrality* are the ones currently in vigor in Switzerland.

Benevolent Neutrality[50]	A policy whereby the proclaimed neutral State has some favorable policies, such as trade, toward one of the belligerents.
Qualified Neutrality[51]	A policy whereby a State abstains from active participation in the hostilities to discriminate in favor of the victim State.
Armed Neutrality	A policy whereby a neutral State is willing to defend its neutrality with armed means.
Active Neutrality	A policy whereby a neutral State recognizes its responsibility for international peace and actively collaborates as a trustworthy third party.
Differential Neutrality	A policy whereby international organizations may be joined, and economic sanctions may be followed if the international community widely accepts them. No military sanctions are to be followed. The aim is to remain unbiased toward any power.
Integral Neutrality	A very strict and absolute interpretation of neutrality with isolationist aspects. No supranational organizations can be joined, and no economic or military sanctions can be followed.

Table 3: Examples of different neutrality policies

[50] As practiced by the US during the first years of WWI, benevolent neutrality is a contentious foreign policy to hold with regards to International Law. It is generally viewed as a poor excuse for violation of duties of abstention and impartiality. For an analysis of the validity of benevolent neutrality or non-belligerency, see Heintschel von Heinegg, supra note 25. For a different view, see Ronzitti, N. (2005) *Italy's Non-Belligerency during the Iraqi War*, in International Responsibility Today: Essays in Memory of Oscar Schachter, Martinus Nijhoff, Leiden, pp. 197–207.

[51] As argued by Boothby and Heintschel von Heinegg, *supra* note 11, "The practical relevance of the concept is limited to situations in which the UN Security Council has authoritatively identified the aggressor State by a (binding) decision based on Chapter VII of the UN Charter. Without such identification, it is almost impossible to identify the aggressor and the victim of aggression. In the Falklands/Malvinas War (1982) and in the Iran–Iraq War (1980–88), both parties to the respective conflicts claimed to be the victims of aggression and to be exercising their inherent right of self-defence".

2 Analogies

As the law of neutrality has not developed much since the 1907 Hague Conventions, the interpretation of how it applies to computer networks involves the use of analogies to the first set of modern information and communication technologies (ICTs) explicitly discussed in it: the telegraph, the telephone, and the radiotelegraph.[52] Moreover, there is a question of whether and how computer infrastructure or code can be categorized as an "apparatus for the purpose of communication," "munitions of war," or "corps of combatant," which are also terms used in the Hague Conventions. All legal opinions on how to apply the law of neutrality to cyberspace, including the Tallinn Manual and the published views of individual States, rely on such analogies and categorizations.

Hence, a rough understanding of the functioning and social organization of the above technologies is required to see if and how the 1907 neutrality conventions might be applied by analogy. **Logical coherence would indicate that any analogy to the telegraph, the telephone, and the radiotelegraph that applies to the Hague Conventions would also apply to other international treaties and the more than 175 years of neutral State practice regarding these technologies.** Therefore, some familiarity with the general legal and political history of these technologies is desirable as well.

This section first provides background on how legal reasoning and analogies work. It then discusses the history of the telegraph, the telephone, and the radiotelegraph, focusing on neutrality and the two World Wars as the most important and extreme test cases for the Hague Conventions. In the final section, the key structural differences and similarities between the analogized technologies are analyzed.

2.1 Background

2.1.1 Legal Reasoning

Legal decision-making is determined by preexisting law and hence requires placing any new event within an existing category. When the category is supported by a written rule with a clear meaning that includes the case at hand, the room for interpretation is limited. However, this is not the case for the Hague Conventions and cyberspace.[53] Legal decisions regarding the applicability of categories are often binary, and membership in different categories can be mutually exclusive. Hence, legal conflicts can boil down to contested categorizations. A classic example is whether the liability of a steamboat company should follow the regimes for trains or that for inns. A modern example is whether Uber is a technology or a transport service, as the latter has licensing requirements.[54]

The view of many legal professionals is that training provides them with a distinct type of reasoning involving formalism and analogical reasoning to argue and decide about contested categorizations. In contrast, legal realists would argue that lawyers and judges are as susceptible to bounded rationality, motivated reasoning, and confirmation bias as any other group.[55] Overall, it seems hard to deny that there is at least some level of social modulation in the interpretation of the law. Hence, **the application and evolution of the law of neutrality in cyberspace are not exclusively informed by the legal sources themselves but also by necessity, feasibility, and the perceived interests of key actors. As such, neutrality policy and the law of neutrality may not always be entirely separable**.

2.1.2 Relational Reasoning

The primary function of **an analogy is to project the reasoner's initial understanding of relationships in a source domain onto a target domain**, thereby allowing for new inferences about the target domain.[56] When talking about activities in cyberspace, scholars, commentators, and policymakers have readily made use of analogies to other domains and technologies. Typical examples range from telephony to mail to television to a library to a photocopier to highways to the high seas.[57] However, over time, as people became familiar with the target domain and less familiar with some of the source domains, the importance of analogies to make sense of the Internet diminished. **The law of neutrality in cyberspace is an exception to this trend, as it relies on a limited set of treaties with very specific language.**

While analogies can be a useful tools, it is important to be aware of their limitations. Analogies can help decision-makers make sense of legal and policy dilemmas. However, they can also be a device to advocate for pre-existing preferences. If used for the

[52] Schmitt, M. (Ed.). (2017). Tallinn manual 2.0 on the international law applicable to cyber operations. Cambridge University Press. pp. 557-558.

[53] The New York Times already noted the lack of clarity of international law with regards to wireless communication and neutrality in 1914. More than a century of technological development has arguably increased this ambiguity. Bartlett, R. (2007*). The World of Ham Radio, 1901-1950: A Social History*. p. 41.

[54] Court of Justice of the European Union. (2017). *The service provided by Uber connecting individuals with non-professional drivers is covered by services in the field of transport*. curia.europa.eu

[55] Spellmann, B. & Schauer, F. (2012). Legal Reasoning. In K. Holyoak & R. Morrison (Eds.) *The Oxford Handbook of Thinking and Reasoning,* pp. 719-735. New York, United States: Oxford University Press. pp. 719 & 720.

[56] The Hague Conventions analogies are an exception in that most people are not actually familiar with the source domain(s); Holyoak, K. (2012). *Analogy and Relational Reasoning*. In K. Holyoak & R. Morrison (Eds.), The Oxford Handbook of Thinking and Reasoning (pp. 234-259) Oxford, United Kingdom: Oxford University Press. p. 234.

[57] Kurbalija, J. (2016). *An Introduction to Internet Governance: 7th Edition*. DiploFoundation. pp. 24-28.

former function, one should not overstate their explanatory power. Specifically, *Khong* cautions against 1) the isolated use of a single analogy without exploring other parallels, 2) remaining vague regarding what structure of the source domain is projected onto the target domain, 3) no discussion of structural dissimilarities, and 4) using analogies as a substitute for proof.[58]

2.2 Information- and Communication Technology

2.2.1 Telegraph

The electric telegraph was the first electric communication technology and led to a sharp increase in the speed and volume of information exchange across national boundaries. A telegraph operator used a Morse key to manually connect and disconnect a source of electricity to an overhead transmission line. The flow of electricity across a wire translates into written dots and dashes or acoustic dits and dahs. Combinations of these symbols correspond to letters, and a text message sent this way is called a telegram. A telegram had to be paid and deposited at the local telegraph office. Messages could be relayed through multiple offices before arriving at the target office from where it was distributed to the recipient via messenger.

Bringing Together the Electric Currents Dividing Europe

In 1844 Samuel Morse's first line between Baltimore and Washington was opened, in 1858 the first transatlantic telegraph was attempted, and in 1866 a sustainably successful transatlantic line was achieved. In Switzerland, the parliament approved the Telegraph Act in December 1851, which declared the construction of a telegraph network to be a federal matter. As in most countries, the Swiss telegraph network was built and operated by a State monopoly.

Expanding telegraph traffic across boundaries led to coordination issues such as transmission standards, pricing, and allowed languages and ciphers. These were first resolved through bilateral and multilateral treaties, with two distinct groups of States emerging in continental Europe; the German-Austrian Telegraph Association and the Western European Telegraph Union. **Swiss diplomacy had the active goal of "bringing together the two large electric currents dividing Europe,"[59] which happened when the International Telegraph Union (ITU) was founded in 1865 in Paris**. Switzerland contributed to this by maintaining good relations with both France and Austria, even as Austria was somewhat diplomatically isolated at that time[60]. Its proposal to create a permanent bureau for the ITU in Switzerland was accepted due to its neutrality and the respected technical expertise of its Federal Telegraph Workshop.

International Law

The **International Telegraphic Convention of 1875 in St. Petersburg** asserts the right of States to stop private telegrams for vaguely stated concerns. Specifically, Article 8 notes *"*the right to stop the transmission of any private telegram which appears to be dangerous to the security of the State or which would be contrary to the laws of the country, to public order or morality."[61] Article 9 adds that "(e)ach Government also reserves the right to suspend the telegram service for an indefinite period of time, if it deems it necessary, either generally or only on certain lines and for certain kinds of correspondence, on condition that it immediately notifies each of the other contracting Governments*."*[62]

Whereas St. Petersburg explicitly gives the right to restrict, the **Second Hague Conference in 1907** states that a neutral duty to restrict belligerents is only present with regards to military networks built by belligerents and not with regards to public networks.

Article 3 HC V: "Belligerents are likewise forbidden to: (a) Erect on the territory of a neutral Power a wireless telegraphy station or other apparatus for the purpose of communicating with belligerent forces on land or sea; b) Use any installation of this kind established by them before the war on the territory of a neutral Power for purely military purposes, and which has not been opened for the service of public messages."

Article 8 HC V: "A neutral Power is not called upon to forbid or restrict the use on behalf of the belligerents of telegraph or telephone cables or of wireless telegraphy apparatus belonging to it or to companies or private individuals."

The only caveat regarding applying restrictions is that they must be applied impartially to the belligerents. As stated in Article 9 HC V, this explicitly includes the duty to ensure impartial access to privately-owned infrastructure: *"*Every measure of restriction or prohibition taken by a neutral Power in regard to the matters referred to in Articles 7 and 8 must be impartially applied by it to both belligerents. A neutral Power must see to the same obligation being observed by companies or private individuals owning telegraph or telephone cables or wireless telegraphy apparatus."

[58] Khong, Y.F. (1992). Analogies at War: Korea, Munich Dien Bien Phu, and Vietnam Decisions of 1965. Princeton, NJ: Princeton University Press. p. 30.

[59] Balbi, G., Fari, S., Richeri, G., & Calvo, S. (2014). Network neutrality: Switzerland's role in the genesis of the Telegraph Union, 1855-1875. Bern: Peter Lang AG. p. 79.

[60] Ibid. p. 210

[61] Convention télégraphique internationale de Saint-Pétersbourg et Règlement et tarifs y annexés. (1875). itu.int. pp. 7-8.

[62] ibid. p.8

There is no reference to the telegraphic undersea cables in HC XIII. Britain had a dominant position in undersea telegraph cables due to its cable-laying ships and control over the production of the insulating material Gutta-percha, as well as its suitable location for landing transatlantic cables. Already in 1865, France had suggested that all undersea cables should be viewed as neutral infrastructure, even organizing an international conference on the protection of submarine cables in 1884. However, **Britain insisted on belligerents' right to cut undersea cables in war**[63]. Article 15 of the 1884 Convention states "It is understood that the stipulations of the present Convention do not in any way restrict the freedom of action of belligerents."[64] There have been extensive legal writings, particularly by French and German legal scholars[65], that aimed to limit this freedom, but they had limited success.

Article 54 of HC IV puts a restriction on belligerents. However, it only applies to occupied territory: "Submarine cables connecting an occupied territory with a neutral territory shall not be seized or destroyed except in the case of absolute necessity. They must likewise be restored and compensation fixed when peace is made."[66] Article 54 of the 1913 *Oxford Manual of the Laws of Naval War* extends the prohibition to cutting cables in neutral waters connecting neutral States with an enemy State.[67] However, the cables may be cut on the high seas based on "absolute necessity" if the belligerent State conducts a blockade.

State Practice during the World Wars

Britain's cable dominance paid off in the Fashoda Incident (1898), the Boer War (1899–1902), and especially the First World War. Britain was able to cut the only German transatlantic cable immediately.[68] Germany diverted transatlantic traffic through Stockholm thanks to the good offices of neutral Sweden, which added its code on top of the German code before retransmission. However, the transatlantic connection still had to go through Britain, which detected this, protested, and slowed down all Swedish traffic.[69] As a result, the traffic was diverted to a more complex route, which Britain still detected but tolerated. These detours slowed the pace of US–German diplomatic communication. Hence, in 1916, US President Wilson decided to allow the German Embassy to send messages with German codes over the American transatlantic cable.[70] However, the British also spied on the American cable and managed to decipher the so-called Zimmermann-Telegram in 1917. In it, Germany instructed its ambassador to promise Mexico support if it attempted to reclaim territories from the United States of America. The telegram was a major factor in the American declaration of war against Germany.[71]

In Switzerland, the Federal Council mandated control offices that censored international telegrams. This included the restriction to national languages or English and prohibition of the use of ciphers except for the government and foreign embassies.[72] International business traffic suffered severe disruptions. Switzerland suspected the UK of deliberately slowing down Swiss telegrams starting in 1916[73] to give Allied businesses an advantage.[74] The British rejected a proposal for a faster process for economic telegrams sent through a trusted intermediary, the Société Suisse de Surveillance Economique. The annual volume of international telegrams from or to Switzerland fell by 29% from 1913 to 1915–1917.[75]

A postwar attempt by Wilson to push for open and free communications with infrastructure under international control went unaddressed. Instead, the US became increasingly assertive in building up its own telecommunications empire.[76] In the 1930s, telegraphs operated via Morse key became increasingly displaced

[63] Headrick, D. (1991). The invisible weapon: Telecommunications and international politics, 1851-1945. Oxford University Press. p. 76

[64] Convention for the Protection of Submarine Telegraph Cables. (1884). cil.nus.edu.sg.

[65] See e.g., Depelley, J. (1900). Les câbles télégraphiques en temps de guerre.; Kraemer, B. (1903). Die unterseeischen Telegraphenkabel in Kriegszeiten.; Thurn, H. (1903). Das Recht der Seekabel in Kriegszeiten.; Scholz, F. (1904). Krieg Und Seekabel: Eine Völkerrechtliche Studie.; Hennig, R. (1904). Die Seekabel im Kriege.; Jouhannaud, P. (1904). Les câbles sous-marins, leur protection en temps de paix et en temps de guerre.; Müller, H. (1911). Kabel und Seekriegsrecht.; Schuster, L. (1915). Landtelegraphen und unterseeische Kabel im Krieg.

[66] Convention (IV) respecting the Laws and Customs of War on Land and its annex. (1907). icrc.org.

[67] Manual of the Laws of Naval War. (1913). icrc.org.

[68] Headrick, D. (1991). The invisible weapon: Telecommunications and international politics, 1851-1945. Oxford University Press. p. 99.

[69] Friedman, W. & Mendelsohn, C. (1938). The Zimmermann Telegram of January 16, 1917 and its cryptographic background. Washington: United States Government Printing Office. pp. 8&9; Headrick, D. (1991). The invisible weapon: Telecommunications and international politics, 1851-1945. Oxford University Press. p. 168.

[70] Friedman, W. & Mendelsohn, C. (1938). *The Zimmermann Telegram of January 16, 1917 and its cryptographic background.* Washington: United States Government Printing Office. p. 12.

[71] Hugill, P. (1999). Global communications since 1844: Geopolitics and technology. JHU Press. pp. 47-48.

[72] Swiss Federal Council. (1916, May 15). Dritter Bericht des Bundesrates an die Bundesversammlung über die von ihm auf Grund des Bundesbeschlusses vom 3. August 1914 getroffenen Massnahmen. p. 22; The Swiss Postal, Telephone and Telegraph Agency did not accept telegrams in Rumantsch, which only became a national language after a vote in 1938.

[73] Delays of telegrams sent from the UK to Switzerland went from 1 day in January 1916 to 5-6 days in September 1916, for correspondence with the US delays went up to 14 days.

[74] Specifically referring to comments by the British War Minister in the House of Commons on August 8, 1916. Britain created the Ministry of Blockade in 1916, which attempted to strong-arm neutrals into exclusive exports to Britain. This included a telegraphic embargo on the Netherlands from November 1917 to February 1918.

[75] Swiss Postal, Telephone and Telegraph Agency. (1952). Hundert Jahre Elektrisches Nachrichtenwesen in der Schweiz 1852-1952: Band III. p. 1029

[76] Headrick, D. (1991). The invisible weapon: Telecommunications and international politics, 1851-1945. Oxford University Press. pp. 175-183.

by typewriters that automatically translated letters into Baudot code. New networks for telegraphic exchange (Telex) via teletype were built and included automatic routing. Telex offered point-to-point connections based on unique Telex addresses. It also enabled more asynchronous communication as the receiving machine could automatically print the code as text.

In the Second World War, Switzerland again mandated censorship. All international telegrams had to go through censorship offices in Geneva, Lausanne, Bern, Basel, and Zurich. Other international connections were physically disconnected. The same went for all international telex connections.[77] The annual volume of international telegrams rose by 29% from 1938 to 1941 but declined to 12% below the 1938 level in 1944.[78]

2.2.2 Telephone

The telephone achieved commercial viability in 1877 with the patents by Bell and Gray. Importantly, the maximum range of telephone cables was significantly lower than that of telegraph lines, which is why the expansion from city to regional to national and international networks was slow[79]. The first radio-based transatlantic telephone service started in 1927, and the first transatlantic telephone cable began in 1956. Until the 1970s, international phone calls remained a marginal phenomenon compared to local calls due to high costs and limited bandwidth.[80]

To connect the telephone cables variably between two endpoints, they converged at an exchange. Originally, these exchanges were operated manually and almost exclusively by women. The world's first self-dialing exchange began operating in 1892. In Switzerland, the first fully automatic telephone exchange began operating in Lausanne in 1922.

State Practice during the World Wars

The Swiss Federal Council suspended almost all international telephone traffic by physically disconnecting cables and even prohibiting interurban phone calls for private citizens within Switzerland for the duration of the First World War[81]. The annual volume of international calls to or from Switzerland fell by more than 99% from 1913 to 1915–1917.[82]

In the Second World War, international phone calls were again prohibited for private citizens in Switzerland. However, this time key lines were maintained for service. Still, some telephone lines at the border were disconnected, others were changed from automatic switching to manual switching, and censorship offices were instated to check samples of calls.[83] The annual international call volume to or from Switzerland fell by 81% from 1938 to 1940–1944.[84]

2.2.3 Radiotelegraph

Radio communication involves the sending and receiving of signals through electromagnetic airwaves. The first radio experiments by Guglielmo Marconi occurred in 1895, the first radio message across the English Channel in 1899, and the first transatlantic radio transmission in 1901. Importantly, the spark gap transmitters used in these first years could not transmit sounds. Hence, radiotelegraphy relied on Morse code. The early focus of radiotelegraphy was ship communication, and from 1901 on, Marconi was the official supplier to the British Navy.

International Law

At the **Second Hague Conference,** radiotelegraphy appears in the previously mentioned Articles 3, 8, 9 HC V. Contrary to the telegraph and the telephone, which were not possible to use on a ship, radiotelegraphy is also explicitly mentioned in Article 5. HC XIII: "Belligerents are forbidden to use neutral ports and waters as a base of naval operations against their adversaries, and in particular to erect wireless telegraphy stations or any apparatus for the purpose of communicating with the belligerent forces on land or sea."

The **Radiotelegraphic Convention of 1912** stipulates in article 8 that "radio telegraph stations shall be organized, as far as possible, in such a manner as not to disturb the service of other stations of the kind."[85] Article 9 obliges the parties "to accept with absolute priority calls of distress whenever they may come."[86] Furthermore, Article 17 states that "the provisions of

[77] Abteilung für Genie. (1939). Telegraphen- und Telephonverkehr: Mobilisation und Kriegsfall. p. 1.

[78] Swiss Postal, Telephone and Telegraph Agency. (1952). Hundert Jahre Elektrisches Nachrichtenwesen in der Schweiz 1852-1952: Band III. p. 1029.

[79] Hugill, P. (1999). *Global communications since 1844: Geopolitics and technology*. JHU Press. p. 64; Swiss Postal, Tephone and Telegraph Agency. (1952). Hundert Jahre Elektrisches Nachrichtenwesen in der Schweiz 1852-1952: Band III. p. 852.

[80] As of 1952, still close to 99% of phone calls in Switzerland remained domestic. Swiss Postal, Tephone and Telegraph Agency. (1952). Hundert Jahre Elektrisches Nachrichtenwesen in der Schweiz 1852-1952: Band III. p. 1037.

[81] Swiss Federal Council. (1914, December 1). Bericht des Bundesrates an die Bundesversammlung über die von ihm auf Grund des Bundesbeschlusses vom 3. August 1914 getroffenen Massnahmen. p. 23.

[82] Swiss Postal, Tephone and Telegraph Agency. (1952). Hundert Jahre Elektrisches Nachrichtenwesen in der Schweiz 1852-1952: Band III. p. 1036.

[83] Abteilung für Genie. (1939). Telegraphen- und Telephonverkehr: Mobilisation und Kriegsfall. pp. 2&3; Abteilung für Genie. (1939). Telephonverkehr vor, während und nach einer Mobilisation.

[84] Swiss Postal, Tephone and Telegraph Agency. (1952). Hundert Jahre Elektrisches Nachrichtenwesen in der Schweiz 1852-1952: Band III. p. 1037.

[85] International Radiotelegraph Convention. (1912). itu.int. p. 143.

[86] Ibid. p. 143.

articles 1, 2, 3, 5, 6, 7, 8, 11, 12 and 17 of the International Telegraph Convention of St. Petersburgh dated 10th July, 1875, shall be applicable to international radio telegraphy."[87] As such, States have the right to prohibit any private use of radiotelegraphy for security concerns.

State Practice during the World Wars

In the First World War**,** Britain quickly managed to destroy German wireless stations in colonial territories. After US President Wilson's neutrality declaration in 1914, the US insisted that no "unneutral" messages could be sent through wireless telegraph on its territory and that messages had to be sent without codes.[88] This was in line with article 9 HC V. However, in practice, it favored Britain, which could still rely on a secure diplomatic channel for wired telegraphy. The US Navy took over two German-owned radio stations as well as two Marconi-Stations that were caught or strongly suspected to be communicating ship movements to belligerent ships.[89]

In Switzerland, the Federal Council suspended all private radio receiver licenses and only reissued them in 1919, arguing that it could not control international communication via wireless telegraphy[90]. Existing installations had to be rendered inoperable[91]. In 1915 and 1916, the Swiss military entered secret negotiations with Telefunken to build a high-powered radiotelegraphy station that would have enabled direct commercial traffic between the US and Switzerland.[92] However, the project did not materialize.

During and after the First World War **radiotelephony**, using radio waves to transmit analog voice signals, reached maturity. In the 1920s, this led to a boom in **radio broadcasting**, in which a large station transmits music and news to many much smaller radio receivers. In 1922, the US helped set up a commission that looked into rules for radio and aircraft as "new agencies of warfare." The **rules concerning the control of radio in time of war**[93] were drafted in 1923. These rules would have increased neutral duties and broadened the scope of applicability to all communication through electromagnetic waves.[94] For example, article 8 states that "neutral mobile radio stations shall refrain from keeping any record of radio messages received from belligerent military radio stations, unless such messages are addressed to themselves. Violation of this rule will justify the removal by the belligerent of the records of such intercepted messages."[95] However, they were never adopted.

The radio boom also led to a vibrant community of amateur radio enthusiasts. When the Second World War broke out, the US radio amateur organization declared a neutrality policy for all its members.[96] However, the US government, which had argued that it would be "very difficult to monitor this service to guard against deliberate or unintentional breaches of neutrality,"[97] still banned amateur radio operators from international communication in June 1940.[98]

Switzerland had already banned amateur radio operators from sending radio signals in 1939. In September 1940, surrounded by Axis powers, it declared a general prohibition on all sending equipment for "electric, radioelectric, optic or acoustic to transmit signals, images, or sound." Switzerland suspended the radio broadcasting license of the Swiss Broadcast Society (SRG) in 1939 and continued to broadcast under the army's control.

Modern Developments

Telegraph, telephone, and radiotelegraph have undergone three notable modern developments: a unification in governance, an increasing obsolescence, and a major wave of telecommunications liberalization.

Unification: In 1925, the Comité Consultatif International des Communications Telephoniques à Grand Distance was incorporated into the ITU. In 1932, the ITU became the governing institution for all telecommunication technologies, including the telegraph and the radiotelegraph. The International Telecommunications Convention has been amended over the years and complements the ITU's constitution.

[87] Ibid. p. 147.

[88] Wilson, W. (1914). *Executive order of August 5, 1914, regarding unneutral radio messages.*; Wilson, W. (1914). *Executive order No. 2042 of September 5, 1914, regarding Government control of high-powered radio stations*.

[89] Headrick, D. (1991). The invisible weapon: Telecommunications and international politics, 1851-1945. Oxford University Press. pp. 141-144.; Bartlett, R. (2007). The World of Ham Radio, 1901-1950: A Social History. pp. 40-49.

[90] Swiss Federal Council. (1914, December 1). Bericht des Bundesrates an die Bundesversammlung über die von ihm auf Grund des Bundesbeschlusses vom 3. August 1914 getroffenen Massnahmen. p. 23.

[91] Swiss Postal, Telephone and Telegraph Agency. (1952). Hundert Jahre Elektrisches Nachrichtenwesen in der Schweiz 1852-1952: Band III. pp. 269-270.

[92] Schade, E. (2000). Herrenlose Radiowellen: Die Schweizer Radiopolitik bis 1939 im Internationalen Vergleich. Baden, Schweiz: Hier + Jetzt. pp. 86-92

[93] Moore, J. (1924). Rules of Warfare: Aircraft and Radio; Part I: Rules for the Control of Radio in Time of War. In: International Law and Some Current Illusions and Other Essays. New York, Macmillan Company. pp. 211-225.

[94] The ICRC calls the document "Rules concerning the Control of Wireless Telegraphy in Time of War". However, the head of the commission used the term radio and explained: "The phrase is used in both texts as covering (…) all stations which use Hertzian waves transmitted through air, water or earth." ICRC. (n.d.). *Rules concerning the Control of Wireless Telegraphy in Time of War and Air Warfare. Drafted by a Commission of Jurists at the Hague, December 1922 - February 1923*. icrc.org; Moore, J. (1924). *International Law and Some Current Illusions and Other Essays*. New York, Macmillan Company. pp. 224-225.

[95] Ibid. p. 223

[96] Warner, K. (1940, May). It Seems to Us. In: *QST*. p. 8

[97] Federal Communications Commission. (1939). *Sixth Annual Report*. p. 103

[98] Federal Communications Commission. (1940, June 5). *Foreign Amateur Communication Banned*.

These documents do not directly refer to neutrality.[99] However, the broad rights of States that originated with the 1875 St. Petersburg Convention to censor any private communication or suspend international communication are still included in articles 34 and 35 of the ITU Constitution.[100]

Obsolescence: In the 1980s and 1990s Telex began to be displaced by fax machines, e-mails, and SMSs. Landline telephony has been increasingly replaced by mobile telephony, as well as by wired and wireless Internet.[101] Radiotelegraphy is also obsolete.

Liberalization: Europe and other regions liberalized their telecommunications sector in the 1990s. The Swiss Postal, Telephone, and Telegraph agency was split in 1998 into the Swiss Post and Swisscom. In 2006, Swisscom spun off its remaining Telex clients to SwissTelex SA, which declared bankruptcy in 2020.

2.2.4 Cyberspace

Since the early 1990s, the term "cyber" has been used to refer to activities enabled by the Internet, which had recently become commercialized. However, while the Internet is a large part of cyberspace, it cannot be equated with it. After all, cybersecurity and cyberdefense activities include computer networks that are not connected to the public internet or do not rely on IP-networking, such as military networks or industrial SCADA systems. The US government defines cyberspace as a "global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the internet, telecommunications networks, computer systems, and embedded processors and controllers."[102] As such, cyberspace may be equated with the entire set of modern information- and communication technology.[103] However, **in this report, we use the term "cyberspace" more narrowly, following the definition in the Tallinn Manual as "the environment formed by physical and non-physical components to store, modify, and exchange data using computer networks."[104]**

Functioning of the Internet

The Internet is a global public network consisting of about 100,000 computer networks, called autonomous systems, connecting billions of devices. Contrary to early telephone networks, the Internet is not circuit-switched but rather packet-switched. In the former, a dedicated communications channel is established between the parties for the duration of a session. In the latter, the data is split into packets forwarded by routers based on forwarding tables. These tables are dynamic and depend on factors such as available bandwidth, agreements between autonomous systems, and the range of Internet Protocol (IP) addresses that each systems advertises as under its control. Hence, each of the packets can potentially take a different route through the network. Furthermore, the routing protocol between autonomous systems, known as the Border Gateway Protocol, depends on trusting advertised IP ranges and makes it hard for the sender to control the path to the receiver.

Internet History and Governance

The history of general-purpose computer networks begins with the Advanced Research Projects Agency Network (ARPANET), which connected US research institutions from 1969 onwards. As the Internet is the globalization of a US network, parts of it remained under the supervision of the US government until recently. Only in 2016 did the US cede stewardship over the Internet Corporation for Assigned Names and Numbers (ICANN), which coordinates the global Internet's systems of domain names and IP numbers. However, a rift persists between China, Russia, and the West. Western States and tech giants prefer the current multistakeholder model. In contrast, China and Russia argue for a multilateral model, in which the ITU governs the Internet, and the domain name system might be nationalized like telephone numbers, which are assigned nationally with international prefixes.

2.3 Analysis

First-generation ICTs and computer networks have functional similarities, but there are important ways they differ. Table 4 provides an overview that highlights both of these aspects and supports them with numbers. It is also worth highlighting that the Hague Conventions were not designed with modern issues in mind and that analogies can include unintended legal precedents.

2.3.1 Structural Similarities

First, the telegraph, the telephone, and the radiotelegraph were state-of-the-art telecommunication in 1907, whereas computer networks are today's main telecommunication network.

[99] At least in the sense of the Hague Conventions. The texts do contain gender neutrality, carbon neutrality, and technology neutrality.
[100] ITU. (2019). Constitution of the International Telecommunications Union. In: Collection of the basic texts adopted by the Plenipotentiary Conference. pp. 43-44.
[101] In Switzerland it peaked in 2001. Federal Office of Communications. (2020). Transmission of voice and data on private connections (PSTN / ISDN or VoIP) / Number and duration of calls.
[102] National Institute of Standards and Technology. (2021). Cyberspace.
[103] See e.g., Binxing, F. (2018). Cyberspace Sovereignty: Reflections on Building a Community of Common Future in Cyberspace. Springer.
[104] Schmitt, M. (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. p. 564.

Second, this includes text and voice transmission across a distance, the primary functionalities delivered by the telegraph, the telephone, and the radiotelegraph, which are mostly provided via the Internet today. Third, the Internet is also the logical successor of these technologies in terms of propaganda and diplomacy during international armed conflicts. Fourth, it is possible to highlight several technology-specific structural similarities. For example, the telegraph's undersea cable routes overlap substantially with the routes of the data cables that handle well over 95% of international Internet traffic. Similarly, in its early days, the Internet ran on lines initially built for landline telephony. Lastly, the amateur radio community has certain echoes in the technical community of the Internet.

2.3.2 Structural Dissimilarities

First, the telegraph and the telephone were organized as State monopolies in most countries. Second, the volume of data exchange via the Internet is many orders of magnitude above that of previous communication networks. Similarly, computer networks are much more ubiquitous in terms of access and can transmit additional types of data, such as video. Third, the TCP/IP-suite makes it difficult to control the pathway of information. Together, these factors indicate the State's challenges in controlling the Internet to the same degree or in the same way as with previous technologies. For example, manual censorship that preapproves international messages, as was done for the telegraph, is not practical. Instead, neutrality-induced online censorship would have to rely on (semi-) automated processes such as upload filters. Fourth, isolationist approaches to maintaining neutrality would have more negative consequences today due to the data volume. A prolonged disconnection from the rest of the Internet could not only be a violation of human rights but could also create strong negative economic consequences.

Finally, the reason why the governance of computer networks is such a pertinent issue is because sophisticated sets of instructions can be shared over them and that many physical infrastructures are controlled by computers**.** Therefore, **computer network attacks can directly create physical harm and even reach the threshold of an armed attack**. Hence, some computer network activities have invited legal comparisons to kinetic weapons and attacks that do not apply to previous communications technologies. Vice versa, it could be argued that the sections on previous communication technologies do not cover computer network attacks or certain types of private computer networks.

2.3.3 Teleological Issues

The Hague Conventions were designed with problems in mind that do not necessarily correspond to today's issues. For example, the radiotelegraph provisions in HC XIII were written due to belligerent agents in neutral ports informing belligerent warships about the routes of trade and warships of the other side. Hence, from a teleological perspective, HC XIII might rather be mirrored in discussions about satellites, which are the primary means of monitoring ship movements today, than in general cyberdefense politics.

2.3.4 Historical Baggage

As the first 150 years of telecommunications have been State-centered, an international consensus that the international law of the telegraph, telephone, and radiotelegraph applies to computer networks would legitimize the positions of China and Russia in Internet Governance. For example, translating the isolationist neutrality practiced by Switzerland for the telephone and radiotelegraphy to the Internet could imply developing a peacetime capability to operate a national Internet (e.g., local data storage, national domain name system, and disconnection from Internet Exchange Points). However, such efforts are condemned in the West. Similarly, the international law of the telegraph and radiotelegraph includes explicit and wide-ranging rights to censorship based on vague grounds. Moreover, the telegraph, the telephone, and the radiotelegraph are all governed by the ITU, which many Western countries oppose with regard to Internet governance.

2.4 Application

Despite the abovementioned challenges, there is a practical reason to apply the Hague Conventions to computer networks. Namely, it is highly unlikely that there will be any significant update to the law of neutrality in the foreseeable future (see Section 4.5). However, the application should be made with today's practical realities in mind, and analogies should be reduced to the necessary minimum.

The prohibition against erecting *"wireless telegraphy station or other apparatus for the purpose of communicating with belligerent forces on land or sea"* on a neutral's territory and use of any such apparatus established before the conflict that is not open to the public (Article 3 HC V) has been interpreted by the Tallinn manual to apply to computer networks.[105]

[105] The Tallinn Manual states that it is applicable to cyber infrastructure, which it defines as "the communications, storage, and computing devices upon which information systems are built and operate". Schmitt, M. (Ed.). (2017). Tallinn manual 2.0 on the international law applicable to cyber operations. Cambridge University Press. pp. 558 & 564.

However, as they may also be subsumed under the category "*other apparatus for the purpose of communicating,"* this does not require an explicit analogy to wireless telegraphy. Similarly, the prohibition "to erect wireless telegraphy stations or any apparatus to communicate with the belligerent forces on land or sea" in neutral ports and waters (Article 5 HC XIII) can be applied through the open-ended term. Whether the phrasing in Article 3 HC V and Article 5 HC XIII contains a legal loophole for military equipment exclusively used to communicate with forces in air and space has not been addressed in the literature.

Article 8 and 9 HC V cannot be applied to cyberspace without analogies. Article 8 HC V clarifies that neutral States do not have to restrict belligerents' access to "telegraph or telephone cables or of wireless telegraphy apparatus belonging to it or to companies or private individuals." Article 9 HC V contains the impartiality principle with the explicit extension that "a neutral Power must see to the same obligation being observed by companies or private individuals owning telegraph or telephone cables or wireless telegraphy apparatus."

The experts drafting the HPCR were convinced that a similar rule could be extrapolated to the Internet[106] without mentioning other computer networks. Similarly, a majority of the experts drafting the Tallinn Manual agreed that "using a public, internationally and openly accessible network such as the Internet for military purposes does not violate the law of neutrality" based on the understanding that Article 8 HC V applies to "cyber communication systems."[107] The manual does not clarify why the qualifier "public, internationally and openly accessible network" is used[108] and whether that is a necessary condition.[109] However, one could argue for limitations to the applicability of Article 8 HC V to computer networks based on teleology and structural dissimilarities. Specifically, in the Hague Conference proceedings, Colonel Borel explains that "we are here dealing with cables or apparatus belonging either to a neutral State or to a company or individuals, the operation of which, for the **transmission of news**, has the **character of a public service**."[110]

The other potential limitation of analogies to previous communication technologies in Article 8 HC V, namely the kinetic-equivalent impacts from certain types of cyber communications, is addressed through a second analogy to "munitions of war." Specifically, the Tallinn Manual experts agreed that the prohibition of transporting munitions of war across neutral territory in Article 2 HC V applies to cyber weapons.[111] A majority of the Tallinn Manual experts argued that this does not just apply to physical transports of cyber weapons but also across cyberinfrastructure, with the caveat that the neutral prevention duty only applies when the State has knowledge of the transmission and can take measures to terminate it. This limitation to Article 8 is accepted by legal experts such as *Kastenberg, Kelsey, Melzer,* and *Roscini*, who highlight that Article 8 (HC V) was never meant to allow activities that could qualify as acts of hostility against another belligerent.

In contrast, a minority of the Tallinn Manual experts, the United States of America,[112] and France[113] hold that Article 8 is an exception to Article 2, which means that cyberattacks with kinetic-equivalent effects through the Internet do not violate neutrality. This point of view is informed by the fact that both neutral and belligerent States may find it hard to prevent the routing of a cyber operation through a neutral State's territory.

Unfortunately, legal scholars have not clarified whether the source domain of the analogy in Article 8 HC V is the telegraph, the telephone, the wireless telegraph, or the aggregate of all of them. However, logically, any analogy that applies to Article 8 HC V must also apply to Article 9 HC V. Importantly, as the Swiss delegation in 1907 noted Article 6-9 HC V are clarifications and do not have the purpose of providing an exhaustive list and do not allow an inference that non-mentioned aspects are allowed respectively prohibited.[114] Consequently, rejecting the applicability of Article 8 HC V to cyber communications systems would increase legal ambiguity, but it would not imply a positive duty for neutrals to restrict networks to belligerents.

Lastly, regarding submarine cables, the 1884 Convention that acknowledges belligerents' rights to cut undersea telegraph cables specifically refers to

[106] Program on Humanitarian Policy and Conflict Research. (2009). Manual on International Law Applicable to Air and Missile Warfare. p. 52.

[107] Schmitt, M. (Ed.). (2017). Tallinn manual 2.0 on the international law applicable to cyber operations. Cambridge University Press. pp. 556 & 557.

[108] The term Internet itself is defined in the manual as "a global system of interconnected computer networks that use the Internet Protocol suite and a clearly defined routing policy", which arguably includes parts that are not publicly, internationally, and openly accessible.

[109] The term cyber system is defined in the glossary as a synonym for computer system, so neither the analogy nor Article 8 are the source. The likely source is Article 3b, but this only refers to the military use of infrastructure *built by a belligerent*, whereas the wording of Article 8 includes all communications systems.

[110] Brown, J. (1920). *The Proceedings of the Hague Peace Conferences: The Conference of 1907: Volume I: Plenary Meetings of the Conference*. New York, United States: Oxford University Press. p. 141.

[111] Defined as "cyber means of warfare that are used, designed, or intended to be used to cause injury to, or death of, persons or damage to, or destruction of, objects, that is, that result in the consequences required for qualification of a cyber operation as an attack.

[112] "This rule [Article 8 HC V] would appear to be applicable even if the information that is being routed through neutral communications infrastructure may be characterized as a cyber weapon or otherwise could cause destructive effects in a belligerent State (but no destructive effects within the neutral State or States)." Department of Defense. (2016). *Law of War Manual.* para. 16.4.1 / p. 1020

[113] France (2019). *International Law applied to Operations in Cyberspace.*

[114] Schlussbericht der schweizerischen Delegation. (1907). p. 99

"submarine telegraph cables." In contrast, the documents that put some restrictions on cable-cutting refer to "submarine cables," which can be very easily framed as a category meant to entail all submarine cables, including those for the telephone and the Internet.

	Telegraphy	Telephony	Radiotelegraphy	Computer Networks
Economic Regulation	State monopolies on land, British firms dominate undersea cables	Mostly State monopolies	Commercial duopoly (Marconi, Telefunken)	Many commercial Internet service providers, a limited number of hardware companies
Annual Volume of Communication *Data does not include the United States.	World* (1907): 36.8M int. telegrams sent. [115] Switzerland (1907): 1.1M int. telegrams sent, 1.2M received, 1M transit[116]. 95% of connections remained in Europe.[117]	World* (1907): International calls unknown; ca. 360 M interurban calls.[118] Switzerland (1907): 351'000 int. calls limited to 3 minutes. No transit.[119] 100% of connections remained in Europe.	World* (1909): 100'000 radiotelegrams (overall).[120] Switzerland (1907): No civilian licenses. Swiss Army uses it to connect Alpine forts.[121]	World (2021): 3 **zettabytes of Internet traffic** (estimate; overall).[122] Switzerland (2019): 877 petabyte (mobile data, overall), wired traffic unknown
Penetration *Data does not include the United States.	World* (1907): 205'000 telegraphs (0.001% of pop.) Switzerland (1907): 2057 telegraphs (0.06% of pop.)[123]	World* (1907): 7.329 M telephones[124] (0.4% of pop.) Switzerland (1907): 57'290 subscribers (1.6% of pop.)	World* (1907): 322 stations, mostly on ships (0.00002% of pop.)[125] Switzerland (1907): 0 (0% of pop.)	World (2020): 4.66 B Internet users (59.5% of pop.) Switzerland (2020): 8.28 M Internet users (**96% of pop.**)
Routing	An international telegram in 1907 involved several human intermediaries.	An international call in 1907 involved several human intermediaries.	Direct connection between two antennas or limited number of relays	Automated routing. **Path of data not fully controllable for sender or receiver.** Domain name system is globalized with private institutions.
Types of Data	Text	Voice	Text	Text, voice, photo, video, **executable files**.
Belligerent Use	Coordinating friendly troops, propaganda / disinformation, diplomacy	Coordinating friendly troops, diplomacy	Coordinating friendly troops, reporting enemy ship movements, diplomacy (WW2: agents, propaganda)	Coordinating troops, enemy location, propaganda, **disabling military equipment / critical infrastructure**, diplomacy

Table 4: A comparison of telegraphy, telephony, and radiotelegraphy, as existent in 1907, with modern computer networks

[115] ITU. (1909). Statistique Générale de la Télégraphie dressée d'après des documents officiels par le Bureau International de l'Union Télégraphique: Année 1907.
[116] Swiss Postal, Telephone and Telegraph Agency. (1952). Hundert Jahre Elektrisches Nachrichtenwesen in der Schweiz 1852-1952: Band III. p. 1029
[117] Swiss Postal, Telephone and Telegraph Agency. (1952). Hundert Jahre Elektrisches Nachrichtenwesen in der Schweiz 1852-1952: Band III. p. 1030
[118] ITU. (1909). Statistique Générale de la Téléphonie dressée d'après des documents officiels par le Bureau International de l'Union Télégraphique: Année 1907.
[119] Swiss Postal, Telephone and Telegraph Agency. (1952). Hundert Jahre Elektrisches Nachrichtenwesen in der Schweiz 1852-1952: Band III. p. 1036
[120] ITU. (1912). Statistique Générale de la Radiotélégraphie dressée d'après des documents officiels par le Bureau International de l'Union Télégraphique: Année 1909.
[121] Swiss Postal, Telephone and Telegraph Agency. (1952). Hundert Jahre Elektrisches Nachrichtenwesen in der Schweiz 1852-1952: Band III. pp. 423 & 424
[122] Equivalent to about 40 quintillion telegrams, assuming an average length of about 80 characters (=80 bytes), or to 260 trillion calls, assuming 64 kbps for digital telephony and 3-minute phone calls.
[123] Swiss Postal, Telephone and Telegraph Agency. (1952). Hundert Jahre Elektrisches Nachrichtenwesen in der Schweiz 1852-1952: Band III. p. 1022
[124] ITU. (1965). From Semaphore to Satellite. p. 219
[125] ITU. (1908). Statistique Générale de la Radiotélégraphie dressée d'après des documents officiels par le Bureau International de l'Union Télégraphique: Situation a la Date du 30 Juin 1908.

3 The Law of Neutrality in Cyberspace

This section discusses the application of the core principles and rules of the law of neutrality to cyberspace and cyber operations based on a review of State *Opinio Juris* and academic literature.

As of autumn 2021, twenty-three countries published their official views on international cyber law: Australia, Brazil, China, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Iran, Israel, Italy, Japan, Kazakhstan, Kenya, the Netherlands, New Zealand, Norway, Romania, Russia, Singapore, Switzerland, the United Kingdom, and the United States of America. These legal opinions take various formats, such as official dedicated statements, speeches, updated war manuals, annexes to policy documents, or responses to parliamentary inquiries. The following paragraphs are based on a review of over fifty publicly available documents (see Annex E).

Academia has developed an interesting, albeit small, body of literature on the application of the law of neutrality to cyberspace. In the wake of the 1999 *US DoD Assessment of International Legal Issues in Information Operations*, a few precursor scholars discussed the matter further and in more detail, including *Walter G. Sharp* and his 1999 book, *Cyberspace and the use of force,*[126] and *George K. Walker* and his 2002 piece on *Information Warfare and Neutrality.*[127] Both explored existing neutrality principles in different domains– i.e., land, sea, and air – in search of analogies (Section 2). However, the bulk of the academic debate and activity on neutrality in cyberspace has occurred between 2008 and 2015/16, with a resurgence in 2021.[128] This unsurprisingly corresponds with a period of general interest around international cyber law and cyber-conflict. Throughout this period, a core group of mostly Western legal scholars[129] and sometimes technologists have extensively addressed neutrality in cyberspace. Of particular note are *Danielle Higson, Eric Talbot Jensen, Stephen Korns, Joshua Kastenberg, Jeffrey Kelsey, Wolff Heintschel von Heinegg, Michael Schmitt, Nils Melzer, Jason Healey, David Turns, Marco Roscini,* and *Noam Neuman*. Many of these are also members of the International Group of Experts involved in compiling the Tallinn and Oslo Manuals.

Based on analogies and references to the Hague conventions and UN Charter, the *Tallinn Manual* outlines how the law of neutrality can be applied to the cyber context (see Annex C). It was prepared at the invitation of NATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE). The first version was published in 2013, and, in 2017, an updated and revised version was published. Both were edited by the American *Michael Schmitt*, a scholar at the Military Academy at West Point. It does not express the official opinions of any States or organizations, and it is not legally binding. However, it has shaped normative and legal debates considerably.

The *Oslo Manual on Selected Topics of the Law of Armed Conflicts*, published in 2020, also covers how the law of neutrality applies to cyberspace (see Annex C). Supported by the Norwegian Ministry of Defense, the manual was led and edited by Israeli law professor Yoram Dinstein and retired Norwegian Judge Advocate General Arne Willy Dahl. It aimed at addressing some of the 2009 *HPCR Manual*'s shortcomings. The group of fifteen experts, most of whom were also part of the HPCR and Tallinn processes, decided to go beyond air and missile warfare and include issues dealing with outer space and cyberspace.

The following subsections are structured along the aspects of the law of neutrality rather than along documents, authors, or countries. They first examine the general applicability of international law, international humanitarian law, and the law of neutrality to cyberspace (Section 3.1). They then discuss the duties of neutral States (Section 3.2), the duties of belligerent States (Section 3.3), and, finally, the remedies following a violation of neutrality (Section 3.4).

3.1 Applicability to Cyberspace

3.1.1 International Law

The application of international law to cyberspace has been a central issue of academic and legal debate for

[126] Sharp. W. G. (1999). *Cyberspace and the Use Of Force*. Ageis Research Corp. pp. 129-33

[127] Walker, G. (2002) "Information Warfare and Neutrality", *International Law Studies*, 76. pp. 1079-1202.

[128] Neuman, N. (2021) "Neutrality and Cyberspace: Bridging the Gap between Theory and Reality". *International Law Studies*, 97, pp. 765-802.; See Dahinden, M. (2021). Schweizer Neutralität im Zeitalter der Cyberkregsführung. ICT4Peace

[129] Higson, D. (2016). "Applying the Law of Neutrality While Transitioning the Seas of Cyberspace," American University National Security Law Brief, Vol. 6, No. 2; Jensen, E.T. (2012). "Sovereignty and Neutrality in Cyber Conflict", *Fordham International Law Journal*, pp. 815; Kastenberg, J. (2009). "Non-Intervention and Neutrality in Cyberspace: An Emerging Principle in the National Practice of International Law" *Air Force Law Review*, 64; Kelsey, J. (2008). "Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare", 106 *Michigan Law Review* 1427; Kastenberg, J. & Korns, S. (2009). "Georgia's Cyber left Hook", *US Army War College quarterly* 38(4) 2009; Melzer, N. (2011). Cyberwarfare and International Law, UNIDIR; Heintschel von Heinegg, W. (2013). Territorial Sovereignty and Neutrality in Cyberspace, Naval War College International law Studies, 89, 2013; *supra* 17 and 26; Healey, J. (2012). When "Not My Problem" Isn't Enough: Political Neutrality and National Responsibility in Cyber Conflict, in 2012 4th International Conference on Cyber Conflict, Tallinn, Estonia; Turns, D. (2015). "Cyber war and the law of neutrality," chapter in: Research Handbook on International Law and Cyberspace, chapter 18, pages 380-400, Edward Elgar Publishing; Roscini, M. (2014). Cyber operations and the Law of Neutrality, chapter in: Cyber operations and the use of force in international Law, chapter 5, Oxford publishing.

many years. The two underlying issues are that most international treaties do not explicitly refer to computer networks and that cyber activities are less contained in or bound to a specific territory than other activities.[130]

Nowadays, there is a broad consensus among States that international law applies to cyberspace**.** This stance has been supported by several international organizations such as NATO, ASEAN, the G20, the EU, the OAS, and most States.[131] The latest OEWG report was the first international document negotiated by a large number of States to acknowledge this stance, explicitly stating "that international law, and in particular the Charter of the United Nations in its entirety, is applicable and essential to maintaining peace and stability and promoting an open, secure, stable, accessible and peaceful ICT environment."[132]

Before this endorsement by the international community, the (initially small) UN Government Group of Experts on Advancing Responsible State behavior in Cyberspace in the Context of International Security (UN GGE)[133] recognized the applicability of international law[134] as early as 2013. The group's 2013 report stated "State sovereignty and international norms and principles that flow from sovereignty [apply] to State conduct of related activities."[135]

The subsequent 2015 UN GGE report[136] built upon these initial results and (re)emphasized the importance of international law, the UN Charter, and the principle of sovereignty as the basis for increased security in the use of information and communication technologies (ICTs) by States.[137] With a similar wording to the OEWG, the UNGA confirmed the findings of the 2013 and 2015 reports in 2018[138].

Just recently, the UN GGE's 2021 report[139] underscored and, for the first time, reaffirmed several core principles of international law in cyberspace, including:[140] sovereign equality; the settlement of international disputes by peaceful means; refraining from the threat or use of force against the territorial integrity or political independence of any State; respect for human rights and fundamental freedoms; and the non-intervention in the internal affairs of other States

3.1.2 International Humanitarian Law

The 2015 GGE report also recognized the applicability of the IHL's fundamental principles of humanity, necessity, proportionality, and distinction to the conduct of hostilities in and through cyberspace – albeit without recognizing IHL per se (due, in part, to China's disagreement).[141] Unlike previous reports, the 2015 report differentiated between binding international law and voluntary, nonbinding norms for conduct in cyberspace. The UN General Assembly (UNGA) subsequently endorsed the 2013 and 2015 reports.[142] The 2021 report, after recalling the previous ones, noted for the first time (in the cyber context) that "international humanitarian law applies only in situations of armed conflict."[143] While the reports are nonbinding and thus do not make international law, their endorsements by States within the UNGA represent a form of *Opinio Juris* necessary to the formation of international customary law.

Despite several dissenting opinions, there is thus a growing acceptance among States that IHL fully applies to cyber operations. This includes the premise that all weapons of war and how they are used are generally subject to the provisions and constraints of IHL.[144] This stance has been reiterated in numerous statements, such as by the 2018 Paris Call for Trust and Security in Cyberspace[145]; NATO[146]; the EU[147]; and many States, including the US,[148] the Netherlands, France, the

[130] Jensen, E.T. (2015). "Cyber Sovereignty: The Way Ahead" *Texas International Law Journal*, 50, 276–304.; Kanuck, S. (2010). "Sovereign Discourse on Cyber Conflict Under International Law". *Texas Law Review,* 88, 1571–1598.

[131] E.g.,: ASEAN (2018). ASEAN Leaders' Statement on Cybersecurity Cooperation; United Nations General Assembly (2015). Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security; NATO (2016). Warsaw Summit Communiqué; EU (2018). EU Statement – United Nations 1st Committee: Thematic Discussion on Other Disarmament Measures and International Security

[132] See para. 34 OEWG (2021). Final Substantive Report

[133] The GGE is a body established in 2004 by the UN Secretary-General with a mandate from the UN General Assembly to study, among other things, how international law applies to States' cyber activities, with a view to promoting common understandings. It was formerly known as the GGE on Developments in the Field of Information and Telecommunications in the Context of International Security.

[134] See para. 19 UN GGE (2013). Notes by the Secretary-General

[135] Ibid. para 20.

[136] See UN GGE (2015). Note by the Secretary-General

[137] Ibid para. 24. & 25. Interestingly, the report also notes that "State sovereignty and international norms and principles that flow from sovereignty apply to the conduct by States of ICT-related activities and to their jurisdiction over ICT infrastructure within their territory." (para. 27)

[138] See e.g., UN GA (2018) Resolution 73/266

[139] UN GGE (2021). Note by the Secretary-General

[140] Ibid. para. 70.

[141] Supra note 40. para. 28. D.; Achten, N. (2019). New U.N. Debate on Cybersecurity in the Context of International Security" Lawfare.

[142] See UNGA (2014). Resolution A/RES/68/243; UNGA (2015). Resolution A/RES/70/237

[143] UN GGE (2021). Note by the Secretary-General, para 71(f)

[144] Schmitt, M. (2019). *France Speaks Out on IHL and Cyber Operations: Part I*, Just Security; Legal Scholars often refer to article 36 AP I

[145] Paris Call (2018).

[146] See NATO (2014). 2014 Wales Summit Declaration; NATO (2016). 2016 Warsaw Summit Declaration; NATO (2016). 2016 Cyber Defence Pledge

[147] EU, *supra* note 131.

[148] Interestingly, during his Keynote address to the 2020 US Cyber Command Annual Conference, the US DoD's General Counsel Paul Ney also confirms that it is US policy to apply law of armed conflict principles to military cyber operations occurring outside the context of armed conflict (which is a long-standing position). See Ney, P. (2020). *DOD General Counsel Remarks at U.S. Cyber Command Legal Conference* ; Schmitt, M. (2020). *The Defense Department's Measured Take on International Law in Cyberspace*, Just Security

United Kingdom, and Australia. It is even referenced in the chair's summary of the latest OEWG report.[149] Most of the scholarly community,[150] including the experts of the Tallinn Manual,[151] and key IHL institutions, such as the Red Cross (ICRC),[152] also recognize it.

During the 2015 and 2017 UN GGEs, China, Russia, and Cuba had dissenting views on whether IHL is fully applicable to cyberspace.[153] An issue that led to the breakdown of the talks in 2017. Explaining their opposition to the express inclusion of IHL, the Cuban representative stated that "the supposed applicability in the context of ICT of the principles of international law […] would legitimize a scenario of war and military actions in the context of ICT."[154] Similarly, during the 2019 OEWG sessions, China stated that acknowledging the application of IHL in cyberspace would only legitimize cyber operations during conflicts.[155] This position was reiterated in its 2021 position on international rule-making in cyberspace, which stated that: "States should handle the applicability of the law of armed conflicts and jus ad bellum with prudence, and prevent escalation of conflicts or turning cyberspace into a new battlefield."[156]

The OEWG Chair's summary has highlighted this ongoing debate but mentions that "States underscored that international humanitarian law neither encourages militarization nor legitimizes resort to conflict in any domain."[157] This is further underscored by States like Brazil, which reminded that IHL aims to minimize human suffering and provide a minimum level of protection to civilians irrespective of the legality of the armed conflict.[158] The ICRC has commented that this interpretation is "in line with the preamble of the 1977 First Additional Protocol to the Geneva Conventions (AP I), in which States expressed their conviction that nothing in international humanitarian law can be construed as legitimizing or authorizing any act of aggression or any other use of force inconsistent with the Charter of the United Nations."[159]

In line with these dissenting views and their general aversion to new binding international rules, Russia, Kazakhstan, Iran, and China, have not addressed nor explicitly recognized IHL's application to activities in cyberspace in their released *Opinio Juris* on international cyber law.

As for international law in general, the issue in applying IHL to cyberspace stem from the fact that this body of law does not explicitly refer to cyberspace. Hence, it cannot be applied automatically and does not consider the differences between cyberwarfare and traditional kinetic warfare.[160] However, as the Czech statement to the 2020 OEWG session highlights, this does not mean these instruments cannot be applied to cyberspace; "on the contrary, in its advisory opinion of 1971, the International Court of Justice found that an international instrument has to be interpreted and applied within the framework of the entire legal system prevailing at the time of the interpretation. This concept of dynamic, or evolutionary interpretation is also implied in Article 31(3)b of the Vienna Convention on the Law of Treaties."[161]

3.1.3 Law of Neutrality

Despite the longstanding concerns with cyber activities crossing the threshold of armed conflict, the law of neutrality has remained a niche issue in international legal discussions and multilateral declarations.

Nonetheless, at least among like-minded Western States, the growing view is that IHL applies fully to cyberspace. For these States, one could surmise that the law of neutrality, as a part of IHL, fully applies to cyberspace and cyber operations. In practice, however, only six States out of the twenty-three that have published their views on international law in

[149] UN GGE, s*upra* note 139, p. 12

[150] See Rowe, N. (2008). *Ethics of Cyberwar Attacks, cyber war and cyber terrorism* pp. 105-106; Brown, D. (2006). "A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict", 47 *Harvard International Law Journal*, pp. 179-181; Tikk, E., Kaska, K., & Vihul, L. (2010). *International cyber incidents: legal considerations*, CCDCOE pp. 79-80; Starr, S. (2009). *Towards an Evolving Theory of Cyberpower, The virtual battlefield: perspectives on cyber warfare* 18; Schmitt, M. (1999). "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework", 37 *Columbia Journal of Transnational Law*, pp. 885-937; Sharp, *supra* note 126; Wingfield, T. & Michael, J. (2004). *An introduction to legal aspects of operations in cyberspace*; Dormann, K. (2004). *Applicability of the Additional Protocols to Computer Network Attacks*, ICRC, pp. 1-7.

[151] Schmitt, M. & al. (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, pp. 179-208.

[152] ICRC (2019). *Cyber warfare: IHL provides an additional layer of protection.*

[153] Already in the 2015 report, these views led to the decision to avoid express mention of international humanitarian law and instead merely "note" the applicability of the principles of "humanity, necessity, proportionality and distinction."

[154] Cuba (2017). *Declaration by miguel rodríguez, representative of cuba, at the final session of group of governmental experts on developments in the field of information and telecommunications in the context of international security*.

[155] China (2019). *China's Submissions to the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security*.

[156] China (2021). China's Positions on International Rules-making in Cyberspace

[157] See para. 12 OEWG (2021). *Chair's Summary.*

[158] UN (2021). 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, p. 22

[159] ICRC (2021). *Comments by the International Committee of the Red Cross (ICRC)*

[160] Higson, *supra* note 4.

[161] Czech Republic (2020). *Statement by Mr. Richard Kadlčák Special Envoy for Cyberspace Director of Cybersecurity Department*

cyberspace have explicitly acknowledged this in their *Opinio Juris*[162] (see Table 5): Switzerland, the Netherlands, the United States of America, Italy, Romania, and France.[163] No State has explicitly rejected the applicability of neutrality in their *Opinio Juris*. However, as stated in the premise of the Oslo Manual's rules of neutrality in cyberspace, some States believe that the raison d'être of the law of neutrality, and its reliance on the concept of neutral territory, is inconsistent with the characteristics of cyber activities.

The applicability of the law of neutrality to cyberspace has also been explicitly acknowledged in the Oslo Manual, the Tallinn Manual, and, to some extent, the HPCR Manual.[164] While all are nonbinding documents, they have been generally (or specifically) endorsed[165] by numerous States, indicating some level of shared views.[166]

The legal argumentation for the applicability of the law of neutrality to cyberspace hinges on the ICJ's 1996 *Advisory Opinion on the Legality of the Threat or Use of Nuclear Weapons*, where it found "that as in the case of the principles of humanitarian law applicable in armed conflict, international law leaves no doubt that the principle of neutrality, whatever its content, which is of a fundamental character similar to that of the humanitarian principles and rules, is applicable (subject to the relevant provisions of the United Nations Charter), to all international armed conflict, whatever type of weapons might be used."[167] Thus, while there are specific provisions for land, sea, and air warfare, the fundamental principles of the law of neutrality largely apply irrespective of the domain concerned.

A further argument put forward by *Heintschel Von Heinegg* [168] is based on the premise that cyberspace has a physical infrastructure dimension, which is rooted in territoriality and sovereignty. Considering the core protective function of neutrality,[169] the law of neutrality should, by analogy, apply during war-time to protect the cyberinfrastructure located within the territory of a neutral State or that enjoys its sovereign immunity. This could also include other platforms and other objects used by the neutral State for noncommercial government purposes. This view rejoins that of the Tallinn Manual, which underlines the interconnectedness of cyberspace infrastructure and the risk of harm against private or public infrastructure. Switzerland, however, has noted some limitations as to the scope of application of territoriality and the law of neutrality. Indeed, as highlighted in its *Opinio Juris,* "data are not only transmitted via terrestrial and cable channels but also via satellites located in outer space, which puts them outside the scope of application of the law of neutrality."[170]

	Reference to the Application of IHL	**Reference to the Application of Neutrality**
Australia	Yes	No
Brazil	Yes	No
China	Yes	No
Czech Republic	Yes	No
Estonia	Yes	No
Finland	Yes	No
France	Yes	Yes
Germany	Yes	No
Iran	No	No
Israel	Yes	Limited
Italy	Yes	Yes
Japan	Yes	No
Kazakhstan	No	No
Kenya	Yes	No
Netherlands	Yes	Yes
New Zealand	Yes	No
Norway	Yes	No
Romania	Yes	Yes
Russia	No	No
Singapore	Yes	No
Switzerland	Yes	Yes
United Kingdom	Yes	No
United States	Yes	Yes

Table 5: Published State views on the application of international law to cyberspace (refer to Annex D and E for a list of the documents and quotes)

3.1.4 Threshold of Application

Historically, the threshold of application for the law of neutrality, its duties, and obligations has been *War*, which used to require a formal declaration. However, since the 1949 *Geneva Conventions*, this has not been the case as international law shifted from the notion of

[162] These legal opinions take a variety of formats, such as official dedicated statements, speeches, updated war manuals, annexes to policy documents or response to a parliamentary inquiry.

[163] Denmark and Israel have also mentioned neutrality.

[164] Dinstein, Y. & Dahl, A. (2020). Oslo Manual on Selected Topics of the Law of Armed Conflict. Springer.; See Article 168(b) of Program on Humanitarian Policy and Conflict Research at Harvard University. (2009). Manual on International Law Applicable to Air and Missile Warfare.

[165] While generally endorsed, States have also had some reservations to parts of the legal commentary of these manuals.

[166] Heintschel von Heinegg, *supra* note 29.

[167] See Para 89. ICJ. (1996). *Advisory opinion on the Legality of the Threat or Use of Nuclear Weapons.*

[168] Heintschel von Heinegg, *supra* note 29.

[169] i.e. to protect the (territorial) sovereignty of neutral states and their nationals against the harmful effects of the ongoing hostilities, and to protect belligerent interests against any interference by neutral States and their nationals to the benefit of one belligerent and to the detriment of the other.

[170] Switzerland (2021). *Switzerland's position paper on the application of international law in cyberspace,* p. 5.

War to that of *Armed Conflicts.* Thus, the application of the law of neutrality in the cyber context is exclusively dependent on the occurrence of an International Armed Conflict (IAC), presumably whether or not associated cyber operations have already occurred.

Therefore, the key question is this: What is the legal threshold for the occurrence of an IAC, and thus the application of IHL and the law of neutrality? The simplistic answer is any resort to hostilities or armed force between States,[171] be it by kinetic or cyber means, of any intensity. It may even arise if the status of IAC is not recognized by one of the parties.

As remarked by *Roscini*, *jus in bello* does not require a minimum threshold of intensity (of hostilities) to apply. This is also the ICRC's position which argues that IHL applies to any shot fired between States, preventing any claims that the minimum threshold has not been reached.[172] The *Commentary to Article 2 Common to the Geneva Conventions* notably states that "[i]t makes no difference how long the conflict lasts, or how much slaughter takes place, or how numerous are the participating forces."[173]

The underlying questions are thus these: Does any IAC triggers the law of neutrality?; and could a cyber operation could trigger an IAC and, by extension, the law of neutrality? The first question echoes the previous discussion (Section 1.3.1) on the issues of intensity, size, and duration of a conflict and a possible higher threshold for the application of the law of neutrality compared to the law of armed conflicts. Therefore, if one agrees that the threshold for the law of neutrality is identical to that of *jus in bello*, the law of neutrality would thus apply as soon as any hostilities are conducted between belligerents. This means it would apply irrespective of whether it is a standalone cyber operation of low or medium intensity or an orchestrated destructive campaign. However, if one shares *Roscini's* and *Bothe's* views and considers that the law of neutrality only applies to cyber operations associated with an IAC of "significant scope,"[174] as was the case with the 2008 armed conflict between Russia and Georgia, a single hostile cyber operation would not trigger the applicability of *jus in bello* and consequently the law of neutrality.

This latter view leads us to the second question, which has been the topic of rich discussions between scholars and within the international community. The general view is that cyber operations can, in some specific cases, trigger an IAC. Notably, this can happen if they can be considered an instance of *use of force* between two States – which would meet an IAC's minimal threshold. While *jus in bello* and *jus ad bellum* are two separate bodies of laws, one can – potentially but not definitively – refer to the *jus ad bellum* framework, which relates to the general prohibition (Article 2(4) UNC), exceptional legality and definition of *use of force* and *armed attacks*, to inform the analysis and help answer the question.[175] According to the ICJ, the main difference and relationship between the two legal concepts are that the "most grave forms of use of force" (i.e., those amounting to an armed attack) can be distinguished from "other less grave forms."[176] Additionally, an *armed attack* is also a necessary element for exercising self-defense under article 51 of the UN Charter.

To note, the lawfulness of resorting to *use of force* under *jus ad bellum* does not impact the determination of whether or not an IAC exists. Indeed, the constitutive elements of the notions of *armed attack* and *use of force* and triggering act of IAC remain distinct.[177] However, as stated by *Melzer*, it can reasonably be expected and agreed that "(s)tate-sponsored cyber operations qualifying as a use of force against another State would not only fall under the general prohibition of article 2(4) of the UN Charter, but would normally also trigger an international armed conflict."[178]

While no established legal definition exist yet for *use of force* (nor *armed attack)* in the cyber context, several States and scholars endorse the "scale and effect" test laid out in the ICJ *Nicaragua Case* to determine if cyber operations violates the prohibition on the threat or use of force in Article 2(4) of the UN Charter (and thus reach this definition/ and/or threshold).[179] Specifically, under this test, a cyber operation would constitute *armed attack* if its scale and effects were comparable to those of a "traditional" uses of kinetic force or weapons (or even a conventional armed attack) – i.e. in terms of damage or destruction,

[171] 1949 Geneva Conventions Article 2; and ICTY (1995). "Tadić, Case No IT-94-1, Decision on the Defence Motion for Interlocutory Appeals on Jurisdiction." para 70

[172] ICRC. (2011). "International Humanitarian Law and the Challenges of Contemporary Armed Conflicts" p. 7 ; in Roscini, *supra* note 35, p. 251

[173] Pictet J. (1952-60). "Commentary on the Geneva Conventions of 12 August 1949", Vol 3, p 23; Sandoz, Y., Swinarski, C., & Zimmermann, B. (1987). "Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949" para 62.; in Roscini, p. 251, *supra* note 35.

[174] Roscini and Bothe p. 252, *supra* note 35 & 28.

[175] "It is of note that the use of force is not only confined to the "armed force" whereas the notion of armed attack necessarily requires resort to arms" ÖykülIrmakkesen, (2014). *The Notion of Armed Attack under the UN Charter and the Notion of International Armed Conflict – Interrelated or Distinct?*

[176] ICJ, Nicaragua, para.191; ICJ, Oil Platforms, para.51. Judgment of 6 November 2003, (2003) ICJ Rep 161–219, §§ 51, 64.

[177] ÖykülIrmakkesen, *supra* note 187.

[178] Melzer p.6, *supra* note 129.

[179] ICJ (1984). *Military and Paramilitary Activities in and against Nicaragua,* para. 195. It should be noted that in Nicaragua the ICJ employed this test to determine the existence of an armed attack, rather than a use of force.

death, and/or injury of soldiers or civilians.[180] The factors are equally useful and logical when determining whether a cyber operation constitutes *use of force*. To note, some States, such as Italy and Norway, also include the (severe) disruption in the functioning of critical infrastructure to the set of effects in their *Opinio Juris*. Thus, according to this test, mere disruptions or destructions of ICTs not leading to serious physical damage would not qualify and, as such, would – theoretically – be insufficient to reach the necessary minimum threshold to trigger an IAC. Cyber espionage activities would also fail to qualify.[181]

This test is underlined in rules 69 and 71 of the Tallinn Manual and explicitly supported by Brazil, Australia, Italy, Norway, Romania, Singapore, Estonia, New Zealand, Finland, Germany, the Netherlands, France, the United Kingdom, and the United States of America. Similarly, Switzerland has argued that cyber operations can reach the threshold of armed conflicts when they, by their intensity, impact, and duration, are similar to those of kinetic military operations.[182]

Some others, like the Tallinn Manual, France, Singapore, Romania, the United States of America, or France, also underline a case-by-case factor-based approach to determine whether it reaches the levels of a *use of force* (but also *armed attack*). The factors vary from State to State but may include:[183]

- The origin of the operations and military or civilian nature of the operator
- The extent of the intrusion or seriousness of the attack
- The actual or intended effects of the operation
- The immediacy of the effects
- The significance of the damage to the victim State's objects and/or State functioning
- The depth of penetration of the cyberinfrastructure
- The nature of the intended targets
- The indirect and long-term impact

The various international law statements highlight the following general and concrete examples in which cyber operations correspond to the use of force:[184]

- Injury to or death of persons
- Damage to or destruction of objects
- Digital sabotage of a State's financial and banking system, or other operations that cause widespread economic effects and destabilization
- Penetrating military systems to compromise defense capabilities
- Financing or training individuals to carry out cyberattacks against a State
- Interference with the operation of a nuclear reactor, resulting in widespread loss of life
- Disabling of air traffic control systems which results in the downing of a plane
- Opening a dam above a populated area causing destruction
- Targeting of essential medical services
- Operations leading to the destruction of stockpiles of Covid-19 vaccines

Until now, however, there are arguably only a few cyber operations that could have been categorized as use of force – provided that these were conducted and attributed to a State. Arguably, these include: Stuxnet; the 2012 hack against Aramco; the 2020 ransomware against the Dusseldorf hospital (which potentially led to a direct death); and the 2007 Operation Orchard, in which the Israeli defense forces disabled Syrian antiaircraft systems during the air raid of a nuclear facility.[185]

To note, all of these previous international and legal discussions and examples focused on individual cyber operations reaching the threshold of an *armed attack* or *use of force*. However, one could also envision entire campaigns of cyber operations reaching that threshold too. This is at least what NATO communicated in its 2021 Brussels Summit Communiqué, in which it stated, "Cumulative cyber activities might, in certain circumstances, be considered as amounting to an armed attack."[186] This new perspective not only broadens the debate around potential cyber-enabled triggers to an international armed conflict but also has implications for the law of neutrality. If generalized, this view could potentially mean that the law of neutrality could become applicable following several under-the-threshold cyber operations.

Additionally, it is important to consider that the triggering and existence of an IAC is usually determined based on facts rather than the intention of a State to engage in armed action. However, cyber operations pose a serious challenge to the issue of the existence or

[180] Compiled by Roguski, P. (2020). *Application of International Law to Cyber Operations: A Comparative Analysis of States' Views*. The Hague Programs for Cyber Norms.

[181] Pangrazzi, S. (2020). *Self-Defense against Cyberattacks Digital and Kinetic Defense in light of article 51 UN-Charter*. ICT4Peace.

[182] Müller, D. (2021) La Suisse est-elle préparée à une cyberguerre du point de vue de la neutralité?

[183] France (2019). *International Law applied to Operations in Cyberspace*, p. 7; Riedel, N. (2015). *Cyber Security as a Dimension of Security Policy*; Australia (2017) *International Cyber Engagement Strategy*

[184] Roguski, s*upra* note 180; and complemented by a review of documents listed in Annex E.

[185] Ari Gross, J. (2018). *Ending a decade of silence, Israel confirms it blew up Assad's nuclear reactor*, The Times of Israel.

[186] NATO. (2020). Brussels Summit Communiqué

trigger of an IAC, as States are reluctant to comment on their cyber operations. This was the case with US cyber operations against Iranian targets in June 2019.[187] Not all cyber operations would fall under the law of neutrality. Indeed, according to *Higson*, only those sufficiently linked to the IAC would logically be in concerned. Or, as the Tallinn Manual's commentary puts it, "there must be a nexus between the cyber activity in question and the conflict for the law of armed conflict to apply to that activity."[188] How such linkages are to be assessed is up for debate and will probably depend on each case. One could presume that the assessment criterion could be similar to that of a "cyber armed attack," with an emphasis on the target and its strategic relevance to the conflict. Thus, this criterion could also include malicious cyber activities that are less militaristic, such as disruptive cyberattacks by cybercriminals or hacktivists (e.g., Georgia in 2008). The important caveat is that for these attacks to be legally receivable, they need to be attributed to the attackers with proven links of coordination by a belligerent. The law of State Responsibility, however, does not contain generally applicable burdens, standards, or methods of proof.

Regarding the scope of application, France argues that any operations affecting the territory of neutral States – within the nexus of an IAC or triggering one – are subject to the law of neutrality.[189]

Recognizing the general applicability of existing international law, including international humanitarian law and the law of neutrality, is the first step. However, **the more complicated part is to identify how, when, where and to what extent the content of existing laws translates to activities in cyberspace**. As pointed out by the OEWG, **this is likely to develop progressively through a mix of discussions, declarative statements, State practice, and codification.** In the case of the law of neutrality, State practice has historically played a large role with the duties and rules only emerging after years of State practice and court cases, such as the 1871 *Alabama arbitration*[190] or the 1949 ICJ's *Corfu Channel*[191] case.

Identifying both the existence and content of a customary rule of international law usually calls for a review of State practice and legal opinions.[192] Accordingly, identifying customary neutrality rules applying to cyberspace necessitates examining whether there is sufficient, widespread, and consistent State practice accompanied by *Opinio Juris* relating specifically to the applicability and substance of the law of neutrality to cyberspace.[193]

With regard to State practice, **there hasn't been any case yet, in which a State that has publicly claimed its neutrality was violated by a belligerent following a cyber operation.** Similarly, **very few States have publicly articulated their views on how to apply international law to cyberspace. However, this is slowly changing and will probably continue to do so following the recommendation in the final report of the OEWG to publish legal opinions.**[194]

3.2 Neutral Duties

The following paragraphs review the academic debate and State positions on neutral duties in cyberspace. As discussed in Section 1.3.2, rights and duties between the neutral and belligerents are reciprocal, meaning the neutral duties of abstention, prevention, impartiality, and acquiescence correspond to rights for the belligerents. We will first discuss peacetime obligations before delving into those wartime obligations.

3.2.1 Peacetime Obligations

For **permanently neutral States,** some elements of the law of neutrality apply independently of any international armed conflict. Specifically, it entails a duty "**not to accept any military obligations and to abstain from acts which would render the fulfilment of its obligations of neutrality impossible should the armed conflict occur.**"[195] How such **peacetime obligations** are transposed to the cyberspace context remains largely absent from any discussion on neutrality. They must be defined by the Neutrals themselves through their neutrality policies and practices or by the larger international community.

What is clear, however, is that military alliances or other military assistance obligations with cyber elements are generally prohibited for permanent Neutrals. Hence, while NATO membership is out of the question, multilateral cooperation should be permissible, at least during peacetime, and if it does not create any military obligations. Thus, international cooperation on (nonmilitary) cyber matters, such as confidence-building measures, international law

[187] Hrnjaz, M. (2019). *The War report, The United States of America and the Islamic Republic of Iran: an International Armed Conflict of Law Intensity*, Geneva Academy; Grignon, J. (2014). "The Beginning of Application of International Humanitarian Law: A Discussion of a Few Challenges", *International Review of the Red Cross*, 96 (893), 139–162

[188] Tallin Manual 2.0, p.376, *supra* note 151.

[189] Schmitt, M. (2019). *France Speaks Out on IHL and Cyber Operations: Part I*, Blog of the European Journal of International Law.

[190] Arbitration Tribunal (1871). *Alabama claims of the United States of America against Great Britain.*

[191] ICJ (1949). *Advisory opinion on the Corfu Channel Case*.

[192] State practice means sufficient, widespread, and consistent practice by States. Opinio juris means that the State has undertaken the practice with a sense of legal right or obligation.

[193] Neuman, N. (2021). "Neutrality and Cyberspace : Bridging the Gap between Theory and Reality". *International Law Studies*, 97, pp. 765-802.

[194] *OEWG, supra* note 132.

[195] Bothe, M. (2013). The Law of Neutrality, in The Handbook of International Humanitarian Law, 3rd edn, edited by Dieter Fleck (Oxford: Oxford University Press), p. 554.

discussions, or norms building, should be legal for permanent Neutrals, a practice already established by several permanently neutral States. For instance, Switzerland, Finland, Austria, and Sweden actively participate in such multilateral processes without considering it contrary to their neutrality policies or peacetime obligations. This has also been confirmed by the Swiss Government, which, answering to a parliamentary interpellation, provided the examples of the UN and OSCE's consultative and preventive processes and efforts.[196] Neutrality, as a narrative, is also leveraged to promote Switzerland's role as a bridge-builder, such as in its recent *Digital Foreign Policy Strategy*.[197]

A permanent Neutral's participation in NATO's Partnership for Peace or CCDCOE's programs seemingly does not pose any evident or direct issues as per neutrality duties. This is at least the practice and stance taken by most European permanent Neutrals, such as Switzerland, Finland, Sweden, and Austria, which all support, contribute to, and participate in research, training, and capacity building within the CCDCOE.

Despite these stances and the legal consideration that such cooperation frameworks are not technically tied to any military obligations, they might still affect the political credibility of permanent Neutrals. At the same time, they might also contribute to building their capacity and eventually deterring posture. As such, the level of cooperation on cyber issues will probably vary from one neutral State to another, depending on the neutrality posture they decide to take and their national prerogatives and needs.

One of the potential areas of contention regarding peacetime duties of permanent Neutrals is technical or intelligence cooperation either through CERT or MILCERT networks or the membership and participation to rapid reaction forces, such as NATO's or the EU's cyber rapid response teams. The underlying practical issues are twofold: First, permanent neutral States could weaken their neutral credibility by participating in them. Second, a formalized information exchange on threats and vulnerabilities or a technical support mechanism might hinder a Neutral's ability to prevent violations of its neutral duties in a future IAC if there are no predefined ways to "stop" these mechanisms. A potential remedy could be the negotiation and enactment of suspending clauses if an activity threatens neutrality.

For instance, in the event of a cyber operation triggering an IAC, it could be argued that a neutral State sharing threat intelligence or providing a victim with technical assistance could provide an unfair advantage to certain parties and violate its neutral duties once the cyber operation is attributed. This act could also inadvertently drag the neutral State into the conflict. As long as the neutral State only receives information, intelligence, or support without providing anything in return, this would arguably not be the case. However, the practicality and value of having such a one-sided relationship in a network based on trust can be questioned.

Thus, whether such technical cooperation during peacetime should be avoided to dodge eventual breaches of neutrality remains debatable. A maximalist conceptualization and application of permanent neutrality could subscribe to this if one believes the reputational cost is too big compared to the operational advantage. However, most would argue that such cooperation, including with the private sector, is currently widespread and critical, so cutting off would be too costly and unadvisable.

If one refers to State practice in the non-digital domain, such obligations should generally not preclude any commercial endeavors, such as trade deals or e-commerce between a permanent Neutral and another country. An eventual caveat could be the export of dual-use cyber technologies, which could undermine a Neutral's duty of nonparticipation or impartiality once a conflict arises. State practice, however, has demonstrated that permanent Neutrals, such as Switzerland, export weapons during peacetime, including to countries embroiled in NIACs, such as Saudi Arabia.[198]

Lastly, another obligation stems from the *de facto* deference of the law of neutrality to the UN Charter. Accordingly, and as reminded by Italy in its *Opinio Juris*, "Neutral States must abide by the rules and recommendations taken by the UNSC. They may thus not invoke their neutrality to refrain from adopting such measures against the wrongdoer(s)."[199]

3.2.2 Non-participation/Abstention

To guarantee its right to territorial inviolability, a neutral State should ascribe to a negative duty of abstention or non-participation. Transposed to cyberspace, **a neutral State should not engage in cyber activities or activities that directly or indirectly impact cyberspace, in turn supporting the military actions of one belligerent to the detriment of the other**.[200] Thus, this duty would proscribe neutral States from committing any acts of hostilities, such as cyber operations against the belligerents or providing them with military assistance, the provision of cyber weaponry, or the recruitment of a cyber "corps de combatants."

[196] Müller, D. (2021) La Suisse est-elle préparée à une cyberguerre du point de vue de la neutralité?

[197] Swiss Foreign Ministry (2020). Digital Foreign Policy Strategy

[198] See e.g., SECO (2019). *Exportations de matériel de guerre en 2018*

[199] Italy (2021). Italian Position Paper on "International Law and Cyberspace"

[200] Heintschel von Heinegg, *supra* note 29.

The Netherlands[201] and Switzerland[202] (see annex D) are the only States that addressed this duty, albeit succinctly. The Tallinn Manual does not explicitly address this issue in its rules on neutrality.

Direct Participation

The prohibition of any direct participation to the ongoing cyber-enabled IAC is the most obvious consequence of the abstention duty. However, some questions remain as to the type of activities concerned. The Dutch *Opinio Juris* considered *"*any act from which involvement in the conflict may be inferred or acts that could be deemed in favor of a party to the conflict."[203]

It can be safely argued that forceful cyber operations are prohibited as they would amount to direct hostilities, a clear violation of the law of neutrality, in addition to making the Neutral a party to the conflict. However, the case of under-the-threshold or disruptive cyber operations (e.g., to operations, the economy, or infrastructure) is less clear-cut. Whether or not they can be considered as hostilities will probably require a case-by-case analysis where the general rule of thumb would be to consider, among other things, their impact and link to the conflict (e.g., whether the cyber operations directly or indirectly aided military operations or provided an advantage to a belligerent to the detriment of the other).

Linked to that, a further question surrounding this duty is whether it should apply to cyber-enabled influence operations[204] or cyber espionage campaigns by Neutrals against belligerent States. Indeed, while most countries have national criminal laws prohibiting espionage in their territory, international law is less clear on the matter. For instance, international law rarely addresses espionage during peacetime, and cyber espionage even less.[205] Hence, no international rules or treaties technically outlaw either cyber espionage or cyber influence. Similarly, there is nothing in the law of neutrality prohibiting espionage during wartime. Accordingly, one could surmise that such activities by a neutral State are generally not unlawful per se.

Despite this, discussions about the potential prohibitions or protection linked to the concepts and rules concerning sovereignty and territorial integrity abound, and opinions diverge greatly.[206] For instance, *Heintschel* v*on Heinegg* highlights that the general principle of territorial sovereignty includes the prohibition against exercising jurisdiction on foreign territory. Thus, if a cyber espionage operation could be characterized as such, it would violate the sovereignty of the target State. This is not limited to a neutral State targeting another neutral State but would similarly apply to a belligerent State targeting a neutral State. However, that prohibition is of a general character and not part of the law of neutrality per se.

In addition, such targeting may also have a political aftereffect on the neutral State's reputation and credibility if discovered. This might be severe enough to deter the State from such activities. Additionally, the contemporary dependence on foreign ICT and its potential backdoors also entails that any espionage by a neutral State could potentially fall into the hands of a third party. If that party happened to be a belligerent State, it could be seen as creating an unfair advantage or indirectly providing military intelligence.

Importantly, all of these assertions rely on the assumption that the cyber operations can be attributed to a neutral State under a commonly accepted burden or standard of proof as supplied by the customary international law of State Responsibility (Article 4, 5, 8, and 16 ILC ASR).[207] Of note, some States, such as New Zealand and Finland, as well as the Tallinn Manual (Rule 17), have noted that States are under no obligation to disclose the information upon which their attribution of hostile COs to other States is based.

An interesting and specific case that could arise is a cyber-hostile act against a belligerent, originating from a neutral territory or network but seemingly conducted by a neutral individual instead of the Neutral's military or cyber unit. The answer to this situation and the degree to which a neutral State violates its non-participation duty essentially depends on whether this individual does it of their own accord (e.g., as a patriotic hacker supporting one of the belligerents) or at the direction or indication of a State.

The latter case seems straightforward, provided that a direct link of command or coordination between the State and the hacker can be made and proven. Indeed, "(s)tates cannot escape responsibility for internationally wrongful cyber acts by perpetrating them through proxies."[208] The former case is less straightforward. Nonetheless, what is clear under the

[201]The Netherlands (2019). *Letter to the parliament on the international legal order in cyberspace*

[202] Switzerland, *supra* note 170.

[203] The Netherlands (2019). *Annex : International law in cyberspace*

[204] Despite this, there are a number of discrete areas of international law that nonetheless apply indirectly to regulate this activity. These principally relate to the Use of Force (Jus ad Bellum), International Human Rights Law, and the Law of Armed Conflict. Influence Operations are presumptively lawful in each of these three areas provided that such activities do not cross relatively high thresholds of prohibition. See Stephen, D. (2020). "Influence Operations & International Law", *Journal of Information Warfare,* 19(4).

[205] Prochko, V. (2018). The International Legal View of Espionage.

[206] E.g. Ohlin, J. D. (2017) 'Did Russian Cyber Interference in the 2016 Election Violate International Law', *Texas Law Review*, 95, 1579-1598.; Heintschel von Heinegg, *supra* 29.

[207] Namely: organ of the State (Article 4), empowered by law to exercise elements of governmental authority (Article 5), acting on the instructions of, or under the direction or control, of the State (Article 8), and acknowledgement and adoption of the act as the State's own (Article 11). A state may also incur responsibility for its role in aiding or assisting an internationally wrongful cyber operation by another State (Article 16).

[208] Egan, B. (2016). *International Law, Legal Diplomacy, and the Counter-ISIL Campaign*, speech at ASIL.

law of neutrality (Article 17 HC V) is that the hacker would be stripped of their neutral status and the legal protections linked to it. Thus, they could be nominally considered as part of belligerent forces and targeted as such.

Whether or not the infrastructure (e.g., network, hosting servers, devices) the individual relied on to conduct his operation would also be considered as such is an open question. The answer would depend on several other considerations, including whether networks or devices can have a neutral status (similar to an international strait) and lose it, whether it matters if these belong to the attacker or not, and whether a belligerent would violate a Neutral's cyberinfrastructure or territory by targeting the attacker.

Provision of War Material

According to Article 6 HC XIII, **neutral governments are forbidden to directly or indirectly supply belligerents with "war-ships, ammunition, or war material of any kind whatever."** According to most of the literature, this article is broad enough to include metaphoric *cyber weaponry* in the categories of "war materials" and "ammunition." The important caveat is that such a term still lacks any legally agreed-upon definition and remains controversial. In the literature,[209] central defining elements of cyber weapons include considerations about the context of use (e.g., during an active conflict or rivalry); the purpose or intended use (e.g., to manipulate, deny, disrupt, degrade, damage, or destroy information systems, data, or networks), the impact (e.g., physical or digital destruction, death, social, economic or political harm or disruption), and the (dual) nature of the means or tools used (e.g., worms, botnets, specifically designed weaponized code).

However, none of the widely proposed and used definitions consider all these elements. For instance, the commentary on Rule 103 of the Tallinn Manual defines cyber weapons as "cyber means of warfare that are used, designed, or intended to be used to cause injury to, or death of, persons or damage to, or destruction of, objects, that is, that result in the consequences required for qualification of a cyber operation as an attack."[210] Meanwhile, Rid and McBurney conceptualized a cyber weapon as computer code that is "used, or designed to be used, with the aim of threatening or causing physical, functional, or mental harm to structures, systems, or living things."[211]

Thus, depending on the chosen definition and its scope, cyber weapons could include a wide range of "artifacts," ranging from specific, highly sophisticated programs, such as Stuxnet, to more generic, less sophisticated types of attacks, such as the use of botnets for DDoS attacks (e.g., Estonia and Georgia) or ransomware for economic disruption (e.g., NotPetya). More generally, cyber weapons could also include any device, material, instrument, mechanism, equipment, or software that is designed or intended to be used to conduct a cyberattack.[212] In the context of the non-participation duty, this could suggest that the exchange of code, dedicated tools, or discovered vulnerabilities that would enable or allow a belligerent to conduct a cyber operation should be prohibited.

This prohibition refers only to governmental war material exports and does not concern the private sector. Article 7 HC V explicitly states, "A neutral power is not called upon to prevent the export or transport, on behalf of one or other of the belligerents, of arms, munitions of war, or, in general, of anything which can be of use to an army or a fleet." Again, this is only the case provided the neutral does not discriminate between belligerents (Article 9 HC V), seconded by Article 7 HC XIII, which is similarly phrased. In other words, **the freedom of private citizens and companies to trade with belligerent States remains unimpaired** by the abstention duty. The only few restrictions laid out in Article 9 HC V revolve around impartiality (see Sections 3.2.4 and 4.3.2). Historically, this limitation was developed under the significant influence of the US's neutrality policy. However, it has been sustained on shaky grounds due to doubts about the compatibility between the freedom of private trade and proclaimed government neutrality.[213] These doubts might be sustained, if not reinforced, in our age of digital interconnectedness that is reliant on private infrastructure.

Some authors, such as Nasu,[214] have pointed out that, the separation between public and private actors regarding military exports is often blurred nowadays. As *Stone* already critically observed in 1954, "The political, social, and economic functions of modern State governments, especially the growth of governmental trading, have undermined the traditionally fundamental distinction between the duty of neutral governments to abstain from arming a belligerent, and its liberty to permit its private traders to do exactly that."[215] Thus, **today, the assumption that**

[209] E.g., Mele, S. (2014). Legal Consideration on Cyber-Weapons and Their Definition, *Journal of Law and Cyber Warfare*, 3(1). Dewar, R. (2017). *Cyberweapons: Capabilities, Intent and Context in Cyberdefense,* Cyberdefense Trend Analysis, Center for Security Studies (CSS), ETH Zürich.; Wallace, D. (2018). *Cyber Weapon Reviews under International Humanitarian Law*: *A Critical Analysis.* CCDCOE.

[210] Tallinn manual, p. 452-453, *supra* note 151.

[211] Thomas Rid & Peter McBurney (2012) Cyber-Weapons, *The RUSI Journal*, 157(1), 6-13

[212] Wallace, *supra* note 220.

[213] Nasu, *supra* note 40; For a more detailed analysis see Politakis, G. (1992) Variations On A Myth: Neutrality And The Arms Trade, *German Yearbook of International Law*, 455-495.

[214] Nasu *supra* note 40; see also Stone. J. (1954). "Legal Controls Of International Conflict" 364; Friedmann, W. (1964). "The Changing Structure of International Law" 346-348.

[215] Stone, ibid. p. 364.

there is no governmental involvement in the pursuit of economic gains by private actors from the supply of arms or dual-use technology is seemingly untenable.

This is especially true as export control regimes have increasingly regulated private arms and dual-use technologies exports over the last few decades—at national,[216] regional, or international (e.g., the Wassenaar Arrangement[217]) levels. With the advent of ICTs, these regimes have increasingly expanded to cover certain types of cyber weapons.[218]

Germany, however, contends that the private sector trade of weapons under export control rules to belligerents would violate neutrality.[219] However, as Roscini points out, it is unclear whether the German view is accurate regarding customary international law or even the prevailing view in literature. Indeed, one can refer to the commentary of rule 173 of the HPCR Manual to see a dissenting opinion: the "increasing control of exports of arms and other military equipment by States (…) gives no evidence that States consider themselves obliged by the law of neutrality to exercise such control."[220]

Switzerland, meanwhile, has a provision in its export control law for armed material (Article 22 LFMG) that the good concerned can only be exported if it respects its international legal obligations, which has been interpreted as concerning its neutrality duties.[221]

Accordingly, relevant open questions would include: What are cyber weapons? Are cyber weapons part of an export control regime? Should it include legitimate or legal tools, such as pen-testing or surveillance ones? How is the dual-use nature of certain software considered? How can the neutral State in question verify and ensure compliance with it?

The scope of "war material of any kind whatever*"* is not limited to weapons but might also include, for instance, military or threat intelligence. Accordingly, this could lead us back to our previous example regarding CERT cooperation. More precisely, one can wonder **whether a Neutral would be allowed to warn one of the belligerents, within the framework of a regional or international governmental CERT network information exchange mechanism, of an upcoming cyber operation it detected.**[222]

A strict understanding of Article 6 HC XIII would indicate this example violates a Neutral State's abstention duty. However, as *Neuman* pointed out, such reasoning might be impractical and undesirable. Indeed, this reasoning runs the risk of undermining the underlying rationale of these networks, which rely on a high degree of cooperation and transparency between their members to jointly and rapidly respond to cyber threats. Furthermore, requiring each neutral State to refrain from sharing critical information or investigate the source of the threat to ensure it will not affect its neutrality is burdensome, self-defeating, and time-consuming.

Similar interesting questions also emerge when considering commercial CERT networks and their eventual roles and actions during conflicts. Are neutral States liable or responsible for them? Can they lose their neutral statuses by reporting and/or mitigating an ongoing attack on their networks? One potential answer might be *Healey's* concept of "commercial neutrality," in which the private sector provides neutral technical goods by mitigating and neutralizing attacks without considering the origins of such attacks. However, a proper discussion of this concept beyond this study's scope.

In any case, this small example reflects the complexities and contradictions that can emerge from strict analogies, further highlighting the need to consider the practical realities of the cyber domain when working with legal analogies.

Corps of Combatants

During conflicts, governments may use proxies to provide some level of plausible deniability. This is particularly the case in the cyber context (e.g., the involvement of Russian patriotic hackers in conflicts with Estonia, Georgia, and Ukraine). Importantly for the Neutral, article 6 HC V states that the responsibility of the neutral State is not involved in the case of "persons crossing the frontier separately to offer their services to one of the belligerents."

Due to the prevalence of malicious campaigns by Advanced Persistent Threats (APT) and other proxies, there has been some interest, at least in the academic literature, in revitalizing article 4 HC V, which states that **"corps of combatants cannot be formed nor recruiting agencies opened on the territory of a neutral power to assist the belligerents."** Transposed into cyberspace and cyber conflicts, it is possible to highlight a few issues.

[216] See *e.g.*, Arms Export Control Act, 22 USC 2778; Council Regulation (EC) No. 428/2009, OJ L. 134 (May 29, 2009) 1; Export Control Act 2002 (UK); Defence Trade Controls Act 2012 (Australia); or Loi sur le contrôle des biens RS 946.202.1 and the Loi fédérale sur le matériel de guerre, RS 514.51 (CH).

[217] Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, 1995.

[218] For instance, in 2019, the members of the Wassenaar arrangement agreed to control the exports of military grade cyber software. For further details and a historical analysis of the issue, see Ruhohen, J. & Kimppa, K. (2019). "Updating the Wassenaar debate once again: Surveillance, intrusion software, and ambiguity" *Journal of Information Technology & Politics,* 16(2), pp. 169-186.

[219] According to Section 1112 of the German Military Manual, then, "[t]o the extent to which arms export is subject to control by the state, the permission of such export [by private persons] is to be considered as unneutral Service".

[220] HPCR (2009). *Manual on International Law Applicable to Air and Missil Warfare,* p. 399.

[221] Müller, D. (2021) La Suisse est-elle préparée à une cyberguerre du point de vue de la neutralité?

[222] Neuman, *supra* note 205.

First, establishing the degree of government exhortation that qualifies as recruitment can be a difficult task. It becomes even more difficult assuming that the prohibition extends to **online recruitment, where attribution is seemingly harder**.

Second, the scope of article 4 of HC V only covers **groups organized in a military structure**. This is an important consideration when assessing whether patriotic or potentially hired hacking groups composed of neutral citizens could fall under this denomination. For instance, if it is possible to prove that a group of hacktivists is organized hierarchically with a clear chain of command, they might fall under this duty. However, if the hacktivists operate under a decentralized, siloed, or self-imposed structure, they would not. By extension, article 4 HC V would not, for instance, cover lone hacktivists lurking on public or underground forums that decide to act following an anonymous call to action (e.g., Ukraine). These would instead be considered volunteers under international law.

Third, **the situation of individual volunteers that are not members of the armed forces but operate from neutral territory is not expressly regulated by 4. HC V**. Indeed, volunteers should fall under article 6 HC V. However, as pointed out by *Roscini*, it does not envisage the case of hostile acts carried out by volunteers (behind their computers) from the Neutral's territory without them crossing the frontier. Nonetheless, the Neutral's prevention duty under article 5 HC V prohibits Neutrals from allowing any acts of hostilities on their territory without specifying the author of the conduct; one could thus assume or at least consider that the provision could be extended to acts of volunteers operating from neutral territory.[223]

Fourth, the extent to which **recruiting private contractors or mercenaries** by a belligerent in neutral territory is contrary to article 4 depends on whether they were hired to conduct activity amounting to **direct participation in hostilities**. According to Roscini,[224] if this were not the case, the situation would fall under the rules of neutrality regulating the commercial relations between the Neutrals and the belligerents—and would be lawful as long as it is done impartially. Also, while the mere alignment of political goals and operational targeting objectives might be sufficient for political attribution, it is highly likely to be insufficient to trigger a violation of article 4 or be sufficient for a legal attribution.

Lastly, in both cases—corps of combatants or volunteers—the **neutral citizens would lose their status once they commit hostile acts against a belligerent or enlist** (Article 17 HC V). However, there is disagreement on how long they should lose this status. The ICRC has researched the direct participation of civilians in hostilities and held workshops with about forty law experts. The culmination of this process is the *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law*,[225] which limits attacks on directly participating civilians to the period during which the targeted individual engages in hostilities. Schmitt, by contrast, has argued that the ICRC is biased toward humanitarian considerations and that due to military necessity, there can be no such restrictions.[226]

One interesting applied case in this context involves botnets located in a neutral territory attacking a belligerent. According to Roscini, article 4 would be broad enough to include such networks and categorize them as "corps de combatant." According to this view, neutral States would be prohibited from creating such botnets, while laws would prohibit and prevent belligerent botnets from taking over zombie computers in neutral States (e.g., by dismantling them and their command-and-control nodes when they have knowledge of them)[227]. The Netherland's *Opinio Juris* seems to follow this line of reasoning when they state that they must stop belligerents from using botnets on their territory to protect their neutrality. It is debatable whether this represents a common view.

It is difficult to consider botnets organized in a "military structure" as intended by the Hague article. However, one could argue that some botnets with centralized architecture resemble a traditional pyramidal military structure while others (with decentralized architecture) do not. The fault line might need to focus on the relationship between the bot-herder and belligerent military command structure.

Other Support Activities

In his contentious 2012 article on "political cyber-neutrality," Jason Healey provided a non-exhaustive list of other supportive activities that could violate this duty.[228] Excepting those covered in previous paragraphs, it includes:

[223] Roscini p. 258, *supra* note 35.

[224] Ibid.

[225] Melzer, N. (2009). Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law. ICRC.

[226] Schmitt, M. N. (2011). The interpretive guidance on the notion of direct participation in hostilities: a critical analysis. In *Essays on Law and War at the Fault Lines* (pp. 513-546). TMC Asser Press.

[227] Refer to the "actual knowledge" discussion in the prevention duty section for more details. The issue here is nonetheless a question of scope and limit. Should a neutral adopt a maximalist stance and dismantle all botnets it finds on its space or only those that could possibly be used by belligerents. This leads to two additional questions: how to differentiate them? And to what extent is that not already a question of good practice between technical actors?

[228] Healey, J. (2012). When "Not My Problem" Isn't Enough: Political Neutrality and National Responsibility in Cyber Conflict. In C. Czosseck, R. Ottis, K. Ziolkowski (Eds.) *2012 4th International Conference on Cyber Conflict*. p. 27

- Hosting chat rooms that are coordinating a cyber operation;
- Hosting legitimate military or dual-use targets of interest to one of the belligerents;
- Encouragement of attacks by senior leaders;
- Refusing to respond to requests for help.

There has been no real discussion of the validity and enforceability of these suggestions. However, they would largely hinge on the context at hand.

For the first one, a general sense of the law of neutrality and the duty of abstention would argue that if a Neutral were deliberately providing support on State-owned or controlled cyberinfrastructure to a belligerent or mandated a private company to do so, this would violate the State's neutrality. If the chat rooms were hosted by a private company (like most blogs and chat rooms), this would not fall under the abstention duty. The scenario, however, might fall under a Neutral's prevention duty (see next section) and justify the use of remedies by the injured belligerent (see Section 3.4).

The reasoning behind Healey's second suggestion is similar to the first one, except for the nature of the targets of interests. Accordingly, if the hosting is explicitly and knowingly done on a Neutral's cyberinfrastructure to support a belligerent by seemingly shielding it from direct harm, this would be a violation. Echoing our previous discussion regarding botnets, one could imagine that a Neutral deliberately hosting a botnet's control and command on its network that targets a belligerent is such a violation, which would call for remedies by the aggrieved belligerent. Other considerations may need to be taken into account—for instance, whether or not the target is hosted on a Neutral's critical infrastructure and if the target's disabling by a belligerent might cause unproportioned harm to the neutral State.

Healey's last two suggestions are the most contentious of the four—and probably the most misguided too. More than being a purely legal issue, they are political ones that risk directly affecting a Neutral's credibility and posture despite not necessarily being unlawful under the law of neutrality. Regarding the third suggestion, one could argue that such partial political rhetoric is not technically unlawful under the law of neutrality—or at least under the abstention duty—as long as no direct and concrete "support" materializes for one belligerent to the detriment of the other.

Historically, permanent neutrals' representatives have not always been the most impartial in their statements. During WWI, for instance, several Swiss politicians actively voiced their support for one side or the other without *their actions* being seen as a de facto violation of Switzerland's neutrality. What did put Switzerland's neutrality into question was the Grimm-Hoffmann affair, in which a Swiss socialist politician, with the support of the Swiss minister of foreign affairs, tried to negotiate a secret peace deal between Russia and the German Empire. More recently, the explicit rhetorical support for Georgia by the US during the 2008 Georgian-Russian escalation and war arguably did not impact its conflict neutrality status, nor was it called out as a breach of neutrality on the grounds of nonparticipation.

Meanwhile, the last suggestion would again depend on the situation at hand and type of help requested, such as requests to send technical help abroad or address a violation in its territory. The latter would generally fall under the prevention duty and right to remedies. The former, meanwhile, somewhat echoes the previous CERT cooperation debate regarding technical cooperation and the risk of breaching the neutral State's non-participation duty and/or impartiality duty depending on the case at hand. Strictly speaking, there is nothing in the law of neutrality obligating a Neutral to provide such help if the neutral State itself deems the help adverse to its neutral interests or posture.

Considering broader international law, however, a neutral might, depending on the case at hand, be allowed to provide certain types of technical humanitarian assistance[229] without violating its duties under the law of neutrality. For instance, one could envisage a situation where a belligerent State's cyber operation disproportionally targeted an element of its enemy's civilian infrastructure, such as a hospital network, causing a lasting humanitarian crisis. Theoretically, a neutral State could then offer its impartial assistance in mitigating the effects of the attack. According to Article 70 AP1, the offer would not be regarded as interference in the armed conflict or as an unfriendly act[230] and would have to be consented to by the concerned parties. (Cyber) humanitarian relief, while often associated with States with a tradition of neutrality, such as Switzerland, is not directly linked to the law of neutrality itself. An in-depth, inclusive, and international discussion on the subject would be welcomed as well as an opportunity for interested and experienced States and stakeholders to develop the field further.

3.2.3 Prevention

The prevention duty is mainly derived from Article 5 HC V, which states that on land, a Neutral must not allow or tolerate any of the acts referred to in articles 2 to 4 to occur in its territory. Despite its name, the duty is mostly

[229] Humanitarian assistance and access during IAC are for the most part laid out in the 1949 fourth Geneva Convention and the 1977 first additional protocol.

[230] Swiss FDFA (2014). Humanitarian Access in Situation of Armed Conflicts

concerned with countering or attempting to terminate any violation or infringement of its neutrality instead of strictly preventing them. Its modalities are different according to domains, thus opening the door for an adapted and less stringent approach in cyberspace.

For instance, the prevention duty is absolute on land but more flexible in the maritime and air domains. In these latter ones, the neutral State's obligation is one of *due diligence* using the *means at its disposal* (cf. Article 8 and 25 HC XIII and 15 San Remo Manual; Article 42, 46, and 47 Hague Rules of Aerial Warfare). According to these, the neutral State is not required to possess or acquire the latest technology to enforce its neutrality but only enforce it using its available means: An interpretation that very much resonates with the current digital governance debates and concerns, notably regarding the growing digital divide and differences in cyberwarfare and defense capabilities.

In terms of State *Opinio Juris*, the Netherlands, France, the United States of America, and Switzerland have explicitly addressed the duty (see Annex D). Only the Netherlands refers to the fact that "constant vigilance, as well as sound intelligence and a permanent scanning capability, are required" to enforce this duty.[231] Switzerland, meanwhile, highlights some limits to this duty, indicating that, in its view, a targeted approach akin to closing down its airspace "cannot be used for data traffic on the internet." In practice, however, Switzerland already mandates some types of data and traffic restricting. For instance, it mandates DNS censorship by ISPs to enforce its online gambling laws.

According to Rule 152 of the Tallinn Manual, this duty transposed into the cyber context should thus generally mandate that a **neutral State should not knowingly allow nor tolerate the use of its territory and cyberinfrastructure under its exclusive control for the conduct of hostilities by a belligerent**. The Oslo Manual's Rule 32 has similar wording, albeit emphasizing slightly different aspects. It argues that if a belligerent State uses cyberinfrastructure located in neutral territory, "the neutral State must use reasonable means at its disposal to terminate the attack once it becomes aware of it."[232]

The legal discussions differentiate and revolve around preventing or addressing two cases: 1) cyber operations from a neutral's territory or infrastructure and 2) cyber operations that are routed through neutral territory and infrastructure. To note, these discussions echo the ones pertaining to different belligerent prohibitions (e.g., regarding cyber weapons or transmission of military communication) later described in Sections 3.3.3 and 3.3.4.

Cyber Operations from Neutral Territory

Most scholars agree that a neutral State's prevention duty is **conditional on its ability to detect cyber activity and counter it**.

Indeed, it presupposes some knowledge of the violation it must not allow. The literature differentiates between actual and constructive knowledge. As explained by the Tallinn Manual's commentary to Rule 152, "a neutral State has **actual knowledge if its organs have detected a cyber operation conducted by a party to the conflict originating from its territory or if the aggrieved party to the conflict has credibly informed the neutral State** that a cyber operation has been initiated from its territory."[233] Meanwhile, **"constructive knowledge exists in situations in which a State should reasonably have known** in the attendant circumstances of the activity."[234] The commentary to the Oslo Manual's Rule 32 only addresses actual knowledge but is similar to what the Tallinn Manual describes.

State *Opinio Juris* on neutrality in cyberspace does not yet address the issue of knowledge. However, one could refer to the growing *Opinio Juris* on the due diligence principle/obligation in cyberspace to potentially infer their views. To note, France, the Netherlands, Italy, Japan, Norway, Romania, and Estonia argue in favor of such a due diligence obligation in cyberspace. In contrast, the United States of America and Singapore adopt a more cautious approach, questioning the existence of this obligation or calling for more discussions. Others, like Russia, do not (yet) address the issue of due diligence.

Unfortunately, there is no consensus on whether a due diligence obligation only arises from actual knowledge of malicious cyber activities or whether constructive knowledge is sufficient. Some States have, nonetheless, positioned themselves. New Zealand, for example, argues, "If a legally binding due diligence obligation were to apply to cyber activities (…) it should apply only where States have actual, rather than constructive, knowledge of the malicious activity."[235] France, meanwhile, considers both equally, as does the Netherlands and Norway. Finland takes the stance that "responsibility may be engaged in situations in which it should have known about the activities in question." It is nevertheless clear that "it cannot be concluded from the mere fact of the control exercised (…) over its territory (…) that [a] State necessarily knew, or ought to have known, of any unlawful act perpetrated therein" as per the Corfu ruling.[236]

Regarding a Neutral's prevention duty, the difference in the required knowledge leads to some open-ended questions, notably: Does the extension to constructive knowledge imply a duty for the Neutral to

[231] The Netherlands, *supra* note 201.
[232] Oslo Manual, p. 27, *supra* note 164.
[233] Tallinn Manual 2.0, commentary to rule 152, *supra* note 151.
[234] Ibid.
[235] New Zealand (2020). *The Application of International Law to State Activity in Cyberspace,* p. 3
[236] Finland, (2020), *International Law and Cyberspace*, p. 4.

actively monitor the use of cyberinfrastructure on its territory, as per the HPCR Manual, Rule 170(b)? Some legal experts, such as Jensen[237], took the position that it does. The majority of the Tallinn Manual experts, as well as those of the Oslo Manual, argue that **no such continuous monitoring duty (e.g., of Internet traffic) exists.** They highlight that the prevention duty is really a duty to terminate actions, which is legally and conceptually distinct from preventing actions. A duty to actively monitor would entail practical and technical difficulties for compliance and might have undesired consequences. Most States do not have the control or the monitoring capacities over the vast array of private networks and ISPs. Even if they did, the democratic side effects could potentially be concerning.

Regarding **countering activity**, the Tallinn Manual experts[238] and Jensen agree that there is "a duty on the part of neutral States to take all feasible measures to terminate any exercise of belligerent rights employing cyberinfrastructure falling within the scope of Rule 152."[239] The Oslo Manual has a similar wording, to which it specifically adds that "[t]he duty to use all reasonable means to terminate attacks applies to cyberattacks launched by botmasters located in neutral territory."[240]

Some scholars have highlighted several measures that a neutral could adopt to enforce its neutrality: kinetic and cyber. Brown[241] and Jensen, for instance, argue that the neutral State can leverage offensive cyber operations, such as hack backs or counter cyber operations. A complete national shutdown of a neutral's Internet might also be considered. However, this would have drastic consequences for both the neutral's economy and the fundamental rights of its citizens. The only State that has offered a concrete example in this context is the Netherlands, which stated that it would be ready to impede the use of a botnet.[242]

Other scholars, such as Heintschel von Heinegg, emphasized preventative defensive measures, many of which can be considered cybersecurity good practice. This includes network segmentation, encryption, password management, workforce training, firewalls, and anti-viruses; **establishing, developing, and properly funding a national public and military CERT;** and setting up formal frameworks of cooperation with other private or public, national, or international[243] CERTs. It also includes devising and adopting a legislative and international framework allowing for the prosecution of cyber-criminal activities. This could further entail investigative cooperation mechanisms with other governments, including the warring parties and the private sector. Meanwhile, effective response and preventative mechanisms can be expected, such as working with national ISPs to filter and block suspicious systems and distributing protective software to users.[244] To note, these recommendations are increasingly part of the discussions around peacetime due diligence duty in cyberspace.

The **scope of application of the prevention duty is, at a minimum, that of cyberinfrastructure under a neutral's exclusive control**, which refers to non-commercial government cyberinfrastructure regardless of location. This seems to be the position taken by Switzerland, which only mentions preventing belligerent States' use of its shielded and non-publicly accessible military-controlled systems.[245]

At the maximum, it could include any cyberinfrastructure located on its territory and under its exclusive control. This would thus seemingly include private and commercial cyberinfrastructure. France is the only State with such a maximalist position, stating that a neutral "must prevent any use by belligerent States of ICT infrastructure situated on its territory or under its exclusive control" with the exception of communication on ICT networks (i.e., article 8 exception).[246]

To note, according to article 3 HC V, neutral States should be required to prevent a belligerent from using a pre-existing cyberinfrastructure on its territory for military purposes or establishing any new cyberinfrastructure "not open for the service of public messaging" for purely military purposes. According to the Tallinn and HPCR Manuals, however, the use of the Internet for military purposes is legal, even if it involves neutral cyberinfrastructure. As such, a neutral State must not prevent its use by belligerents.

Additionally, the combined effect of Articles 4 and 5 of Hague Convention V imposes an obligation on neutral States not to allow the formation of "corps of combatants" in their territory to assist the belligerents by conducting cyber operations. As discussed in Section 3.2.2, this might come with a few caveats—among others, the fact that this only covers the formation of groups of individuals that are organized in a military structure.

The last issue regarding this prevention duty is belligerent States using neutral territory or infrastructure for cyber espionage/intelligence purposes: To what extent does a neutral State have to

[237] Jensen, p. 822, *supra* note 130.
[238] Its wording of rule 152 includes explicitly the phrase "may not knowingly allow" upon which rests the following reasoning.
[239] Tallinn Manual, *supra* note 151.
[240] Oslo Manual, p. 27, *supra* note 177.
[241] Brown, D. (2006). A Proposal for an International Convention To Regulate the Use of Information Systems in Armed Conflict, 47 *Harvard International Law Journal,* p. 179.
[242] The Netherlands, *supra* note 201.
[243] An important caveat being the previously discussed potential conflicts between international cooperation - e.g. for threat intelligence exchange – and the abstention duty.
[244] Heintschel von Heinegg, *supra* note 29.
[245] Switzerland, *supra* note 170.
[246] France, *supra* note 183.

end or prevent such activities? While there is no definitive answer, one can refer to nonbinding Articles 47 of the Hague Rules of Aerial Warfare for a useful analogy. It specifically states that "[a] neutral State is bound to take such steps as the means at its disposal permit to prevent within its jurisdiction aerial observation of the movements, operations or defenses of one belligerent, with the intention of informing the other belligerent." By analogy, this could potentially mean that a neutral State has a duty to conduct counterespionage, based on the means at its disposal, to prevent belligerents from exploring and observing neutral networks that would allow them to gain intelligence on the other belligerents' wartime actions.

Cyber Operations through Neutral Territory

The so-called "routing question" has been a central issue in the literature. It consists of two parts: First, is the routing of belligerent cyber operations through the infrastructure based in neutral territory a violation of neutrality? Second, is the neutral State under a practical obligation not to allow such routing as part of its prevention duty? The first question will be addressed under belligerent duties in Section 3.3.4, whereas this section focuses on the second part. However, the two are linked because any neutral prevention duty can only arise if the routing of belligerent cyber operations through neutral infrastructure is a violation of neutrality. Hence, this section already introduces a discussion that is relevant to both questions, namely the tension between Article 2 HC V and Article 8 HC V.

On the one hand, Article 2 HC V prohibits belligerents from moving "convoys of either munitions of war or supplies across the territory of a neutral Power." The popular metaphor "cyber weapons" suggests that certain types of software belong to the same category as kinetic munitions of war. On the other hand, Article 8 HC V states **t**hat neutrals are "not called upon to forbid or restrict the use on behalf of the belligerents of telegraph or telephone cables or of wireless telegraphy apparatus." This means that if we fully accept the analogy to the previous ICT and treat cyber operations as mere communications data, their routing through neutral territory is no violation. The consensus is that both Article 2 HC V and Article 8 HC V apply. However, there is no agreement within the scholarship and State *Opinio Juris* regarding which article takes precedence when they intersect. Does Article 2 override Article 8 and prohibit the routing of cyber operations that have kinetic-equivalent effects through neutral territory? Or is it Article 8 that provides the exception to Article 2, meaning only the offline transport of hardware containing "cyber weapons" through neutral territory is prohibited? As these articles stem from the same treaty, the conflict cannot be resolved by prioritizing the more recent or specific law.

However, even If we accept that Article 2 HC V takes precedence over Article 8 HC V, there are not necessarily any practical consequences. As discussed above, the duty of prevention depends on the *means at disposal* of a neutral State and its *actual knowledge* of the neutrality violation. Most scholars assume that a neutral State is unlikely to be aware of a "cyber weapon" passing through its territory and would not have the means to stop it short of directly stopping all traffic coming into its territory. Broadly speaking, there are three coherent positions:

1. The routing of "cyber weapons" through neutral territory constitutes a neutrality violation, and neutral States must take significant steps to prevent it.
2. The routing of "cyber weapons" through neutral territory constitutes a neutrality violation, but there are few or no practical consequences for neutral States.
3. The routing of "cyber weapons" through neutral territory does not constitute a neutrality violation, and neutral States do not have to take any steps to prevent it.

There are relatively few scholars in the first camp. *Kastenberg* argued that a "neutral state…must also, within its capabilities, take action to prevent a cyber attack from transiting its Internet nodes." Explaining that "if a neutral state cannot or does not take action to halt a cyber attack, a belligerent may choose to counter by physically attacking the neutral state's communications infrastructure."[247] Similarly, *Kelsey*[248] argued that belligerents have such a right to countermeasures regardless of the means at disposal test for the neutral prevention duty. However, she also adds that attacked states might find it impossible to trace the route of attacks and hence would not be able to make demands on neutrals for prevention measures. Lastly, *Healey* argued that letting attacks pass through neutral territory violates political neutrality. Therefore, nations in the attack path should "take reasonable steps to mitigate the attack if they can."[249]

The majority of the International Group of Experts of the Tallinn Manual took the position that the transmission of "cyber weapons" across neutral cyberinfrastructure is prohibited. However, it explicitly

[247] Kastenberg, J. (2009). "Non-Intervention and Neutrality in Cyberspace: An Emerging Principle in the National Practice of International Law" *Air Force Law Review*, *64*, 43-64. pp. 56 & 57.

[248] Kelsey, J. (2008). "Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare", 106 *Michigan Law Review.* pp. 1441-45

[249] Healey, J. (2012). When "Not My Problem" Isn't Enough: Political Neutrality and National Responsibility in Cyber Conflict. In C. Czosseck, R. Ottis, K. Ziolkowski (Eds.) *2012 4th International Conference on Cyber Conflict*. p. 27

cautions that "the obligation of the neutral Power to take action to prevent such transmission only attaches when that State has knowledge of the transmission and can take measures to terminate it."[250] *Brown* introduces a distinction between unintentionally and intentionally routing an attack through neutral territory. He argues that only the latter case should be a neutrality violation and adds that the neutral prevention duty is only violated if the neutral State were to actively assist the belligerent in committing the attack.[251]

Today, a lot of the literature and State *Opinio Juris* support the view that a Neutral must not prevent cyberattacks from passing through its cyberinfrastructure and territory at all. This stance is notably supported by the Oslo Manual (rule 33) and the Commentary to Rule 167(b) of the HPCR Manual, which explains that "the mere fact that military communications, including CNAs, have been transmitted via a router situated in the territory of a Neutral is not to be considered a violation of neutrality." Key supporting scholars are the likes of *Sharp*[252], *Tikk*, *Kadri*, *Vihul*,[253] *Schmitt*,[254] and *Jensen*.[255] Other scholars, such as *Döge,*[256] *Melzer,*[257] *Roscini*,[258] and He*intschel von Heinegg*[259] did so under the specific argument that it would be impossible for a neutral State to control and monitor all the data packets and routes effectively. Moreover, even if this were the case, it would be costly financially and socially for the neutral State. Indeed, such widespread monitoring of a Neutral's network could have strenuous implications for democracy and free speech. As a result, many question why neutral States should be the ones to espouse this burden. Adding to this, some have pointed out that even in the case traffic was detected (e.g., with deep packet inspection technologies), the incomplete data packets would make it look "innocuous" and, as such, unreadable.

3.2.4 Impartiality

The impartiality duty, as stated in Article 9 HC V and XIII, provides that the neutral State must apply every restricting measure and prohibition in the context of its neutral duties and rights in a nondiscriminatory manner toward all belligerents.

The Tallinn Manual rules do not explicitly address the duty of impartiality of a neutral. The commentary nonetheless mentions it when referring to Rules 151 and 152, stating that Neutrals can restrict or prohibit access or use of their cyberinfrastructure but must do so impartially (a clear reference to Article 9 HC V). The Oslo Manual explicitly refers to this duty in its Rule 35, albeit in the scope of limiting a belligerent's establishment of cyber communication for nonmilitary communications and the use of its open/public and closed/private cyber communication installations.[260]

The US, Italy, and the Netherlands are the only States that mention and address this duty in their *Opinio Juris*. The US did so twice: in its 1999 *Assessment by the DoD's General Counsel Office*[261] and its 2015 *DoD Law of War Manual*. In the former, it stated, "A neutral Power is not called upon to forbid or restrict [communications], so long as such facilities are provided impartially to both belligerents."[262] In the latter, the impartial provision of access to neutral communication infrastructures is seen as a requirement for the applicability of the Article 8 exception allowing for the transit of data packets. The Italian and Dutch statements, meanwhile, emphasized an equality of treatment between the belligerents to maintain neutrality.[263] They highlighted that the denial of access to their IT systems must be applied equally to the belligerents.

In practice, the duty of impartiality has always been a contentious one. It also has been somewhat neglected by State practice during the recent IAC, such as during the First Gulf War and the Iraq invasion. This is linked to the (re)emergence of policies and legal arguments of *nonbelligerency* and/or *benevolent neutrality*, whereby declared neutral States willingly disregarded their duty of impartiality and non-assistance, only respecting their duty of nonparticipation in the hostilities. This was notably the case with Italy—but also France, Germany, and Ireland—which supported the invasion of Iraq in 2003 by allowing the use of its military bases by the Multi-National Force.[264] In doing this, they hoped to preserve the protection given to neutral States under the law of neutrality while taking a stance and trying to influence the outcome.

Due to the sociotechnical characteristics of cyberspace and activities therein (e.g., attribution issue,

[250] Schmitt, M. (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. p. 557

[251] Brown, D. (2006). "A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict", 47 *Harvard International Law Journal*. pp. 210 & 211

[252] Sharp, *supra* note 126.

[253] Tikk & al. al. *supra* note 150.

[254] Schmitt, M. & Al. (2004). *International humanitarian Law Research Initiative, Computers And War: The Legal Battlespace*

[255] Jensen p. 825, *supra* note 144

[256] Döge, J. (2020). "Cyber Warfare—Challenges for the Applicability of the Traditional Laws of War Regime", *Archiv des Völkerrechts* 48, p. 497.

[257] Melzer p. 20, *supra* note 129.

[258] Roscini, *supra* note 35.

[259] Heintschel von Heinegg p 149, *supra* note 29.

[260] Oslo Manual, p. 28 & 29, *supra* note 164.

[261] Office of the General Counsel (1999). *An Assessment of International Legal Issues in Information Operations,* DoD

[262] As a mark of its time, the example provided with this quote relate mostly to communication satellites.

[263] The Netherlands, *supra* note 201.

[264] Ferro, L. & Verlinden, N. (2018). "Neutrality During Armed Conflicts: A Coherent Approach to Third State Support for Warring Parties", *Chinese Journal of International Law*, 17, pp. 15-43

the opacity of actions, and dual-use technologies), it can be argued that seemingly neutral States might get away more easily with violations of their duties of impartiality in future IACs. *Turns* notably posits that "the nature of the modern global economy and international commercial realities, as illustrated notably by State practice in the Iran-Iraq and First Gulf War, as well as the inherent practical and technical difficulties in the regulation of cyber activity, seem to suggest that this principle may become less important in future applications of law of neutrality—both in the cyber context as in more conventional armed conflicts."[265]

Nonetheless, there are several potential areas of interest for the application of this duty to cyberspace: access to cyberinfrastructure, sanctions, and trade.

Access to Cyberinfrastructure

The first areas of interest are eventual restrictions or prohibitions to use and access neutral cyberinfrastructure, such as public networks. Both the US and the Netherlands have reiterated the obligation for impartiality in that regard, as has the Tallinn Manual in its commentary in rules 151 and 152 and the Oslo Manual in its rule 35.

While neutral States must non-discriminatively restrict their access to their network, the scope and format of such restrictions could vary. They could range from simple limitations of military communications to a complete halt of any traffic originating from the belligerent States. It could also include restricting traffic originating from a belligerent from transiting through servers physically located in a neutral State. The technical and practical value, feasibility, and implications of such measures, including on fundamental rights, will presumably limit their deployment.

A further issue is that of the private sector and individual impartiality. Article 9 HC V provides that "a neutral Power must see to the same obligation being observed by companies or private individuals owning telegraph or telephone cables or wireless telegraphy apparatus." Thus, if one admits that these technologies are analogous (e.g., in function) to cyberspace, the neutral State itself would have to see that private actors respect their impartiality. One could also, potentially and reversely, argue that ICT companies (e.g., hosting companies or ISP infrastructure) situated on a neutral State's territory must also respect (or at least acknowledge) the duty of impartiality vis-à-vis the belligerent parties. How this should take form in practice, however, remains to be debated.

One interesting real-life example is the case of Tulip Systems (TSHost), a private web hosting company based in the US but founded by a Georgian national, during the 2008 Russo-Georgian War.[266] By initially contacting and then providing special access and support to the Georgian foreign ministry, the company seemingly violated its impartiality (and potentially abstention if it is to extend to the private sector). It provided an advantage to the Georgian government while not offering the same access and support to Georgia's belligerent, Russia. Tulip was subsequently targeted by a DDoS attack which, if it had been attributed to Russia, would likely fall into the right of remedy and a lawful reaction to the violation of US neutrality.

This case also opens up a couple of other practical and theoretical open-ended questions. For one, did the US, under article 9 HC V, have a duty to ensure that Tulip Systems provide—or be ready to provide if requested by Russia—the same hosting services as it did to the Georgian? And how could it have done so? Or, to what extent would Russia need to demonstrate that it would not have been able to host a government website in the US to claim that the US violated its neutrality? Meanwhile, if it was Georgia that had initially contacted Tulip system, would the latter have been obligated to offer its services to Russia proactively? Or would it only have needed to service it if Russia had requested this?

Sanctions

The second area of interest regarding impartiality is sanctions. Historically, some Neutrals, such as Switzerland, have abstained from participating in economic sanctions out of fear of impeding its neutral credibility and duties. Other permanent neutrals, such as Sweden, have not always pursued such a strict policy and have regularly participated in the UN or the EU sanction regime.[267] This was notably the case with the UN's sanctions against Rhodesia (now Zimbabwe) from 1965 to 1979. The differences in policies stem, among others, from different interpretations of the law of neutrality and approaches to collective security.[268]

Accordingly, if one subscribes to a strict conceptualization, it could be contended that a neutral State should, during an IAC, be prohibited from adopting any type of cyber sanctions or coercive economic measures intended to, or having the effect of, significantly weakening only one of the belligerents. Cyber sanctions could still be permissible if they are non-discriminatory.

The various historical precedents of Neutrals imposing collective sanctions might indicate that, to some degree, sanctions could also become a tolerated practice, both for wartime and peacetime. An important caveat is that the use of sanctions concerning cyber activities (aka. *cyber sanctions*) is still in its infancy and

[265] Ibid.

[266] See Kastenberg & Korns, *supra* note 129.

[267] Ross, J. (1989). *Neutrality and International Sanctions: Sweden, Switzerland, and Collective Security*. New York

[268] Ibid.

their efficacy remains highly contested.[269] They are notably limited by issues of receivable proof of attribution to the wrongful act against which they are pitted, as well as appropriate target sanctioning.

There are at least two cases where it would be legal for a neutral State to violate its duty of impartiality: as a remedy against a violation of its neutrality by a belligerent and as part of its UN collective security obligations. Regarding the former, one may posit that a neutral State could be entitled to acts of retorsion or countermeasures—including sanctions—depending on the violation. Regarding the latter, it is widely recognized that restrictions on trade between neutral and belligerent States could flow from other obligations, such as UNSC resolutions. This is based on Article 25 of the UN Charter, requiring member States to comply with Security Council decisions, and Article 103 UNC making treaty obligations (such as those from the Hague conventions) inapplicable when Chapter 7 of the charter is invoked. This exception is explicitly re-stated in the Tallinn Manual (rule 154).

Trade

Trade is the last area of interest for impartiality. Historically, trade has been a key driver and function of neutrality. This arguably remains true in the cyber context. Thus, while the law of neutrality does not prohibit neutral States and private companies from maintaining trade relations with belligerents per se, it does insist that they do so in an impartial and non-discriminative way. Accordingly, a neutral State would be entitled to continue its commercial relations with the belligerents and would not have to equalize them in terms of volume. This echoes the common saying of Swiss policymakers that "impartiality and neutrality is not equidistance."

State and company trade of common consumer or digital goods over the Internet (e.g., e-commerce, consumer software, or hardware) should pose no real issues and would thus be allowed. However, as previously mentioned, the trade of some specific types of dual-use or war-oriented digital goods or applications could infringe on neutrality rules (i.e., abstention duty). Export control regimes would, however, regulate such goods. These regimes should generally be applied impartially between the belligerents.

By analogy, Article 9 HC V, referring to Article 7 HC V, also provides a specific clause for ICT companies to trade impartially and to export goods to all belligerents. According to the wording of Article 7 HC, this would even include the supply of "arms, munitions of war, or, in general, of anything which can be of use to an army or a fleet." While many of these could and/or should fall under dual-use export control regimes, it might need to be considered if other goods that might be of "use to any army," such as computer chips, fall under this rule.

However, unequal trade or export control regimes imposed by States and companies are generally a clear violation of the duty of impartiality. By violating this duty, they forfeit their rights and pretenses to economic neutrality and open the door to remedies by the aggrieved party.

The trade impartiality duty is not always respected to the letter. Indeed, neutral States have often approached trade according to realist and survivalist principles, adapting their practices to the economic and geopolitical exigencies of the time.[270] During WWII, for instance, neutral States often had to make themselves useful for the belligerents to stave off the threat of invasion, even if it meant being partial at times. This took the form of various economic concessions on goods, materials, labor provision, or capital.[271]

3.2.5 Acquiescence

The neutral's duty to acquiesce (i.e., to consent) comes into play when a belligerent exercises its right of remedies (Section 3.4) to terminate a violation. It can generally do so when a neutral State fails (or is unwilling) to terminate (or prevent) an exercise of belligerent rights or another violation of neutrality by one belligerent.

The key question here is thus whether it should be considered and applied passively (e.g., silence or inaction), as it has been historically, or whether it also contains elements of a positive duty to cooperate with the aggrieved belligerent. Some scholars, such as *Healey,* posit that neutral States should cooperate with any request for help by an aggrieved party to stop an attack transiting or originating from its neutral territory or infrastructure. Otherwise, the State would risk losing its "political neutrality."

This is, however, not a widely shared, nor discussed, line of reasoning. It also opens up a number of other questions, including: What kind of help is adequate? Should a neutral provide a belligerent with access to its network to stop the attack? On what grounds can it and should it refuse cooperation (e.g., national security, espionage)? What about forcing national (private) operators to act? Could or should national CERTs coordinate and cooperate with the aggrieved State?

[269] E.g, Soesanto S. (2018). *A hammer in search of a nail: Eu sanctions and the cyber domain.* Journal of International Affairs; Moret, E. (2021) *EU Cyber sanctions between effectiveness and strategy*. Global Governance center.

[270] See Golson, E (2011), "The economics of neutrality: Spain, Sweden and Switzerland in the Second World War," PhD dissertation, London School of Economics.

[271] Ibid.

3.3 Belligerent Duties

The following paragraphs review the academic debate on belligerent duties. As discussed in Section 2.4.2, rights and duties between Neutrals and Belligerents are reciprocal—any belligerent duty corresponds to a right for a neutral. This section first discusses the overarching duty to respect the neutral's territory before delving into specific cases of cyber operations against, from, and through neutral territory and infrastructure.

3.3.1 Territorial Integrity of Neutrals

According to the law of neutrality, the primary duty of a belligerent is to respect the territorial integrity of a neutral State (Article 1 HC V and XIII). Belligerents are prohibited from certain actions, primarily conducting any hostilities or exercising their belligerent rights against a neutral State or within its territory. They are also prohibited from establishing bases of operations in neutral territory and from moving troops, munitions of war, or supplies across it. These prohibitions are laid down in international treaties (e.g., Article 1, 2 and 3 HC V; Article 1, 2 and 5 HC XIII) and are considered customary in character.

As with most rules and principles flowing from the law of neutrality, these prohibitions are based on the notion of territoriality and sovereignty, two legal concepts that may not always be adequate in dealing with cyberspace and activities therein (see Section 4.2). Nonetheless, despite some proposals, such as by *Turns* towards changing focus from territoriality to personality, most of the literature and *Opinio Juris* continues to transpose and apply these rules within a strict concept of territoriality.

Switzerland is the only State to explicitly invoke territorial integrity in its *Opinio Juris*, stating that "Parties to the conflict are obliged in turn to respect the territorial integrity of the neutral country."[272] Other States, such as France, Italy, Romania, the United States of America, and the Netherlands, address to varying extents the duties attached to it, including references to Article 1 HC V, but never explicitly acknowledge a neutral country's territorial integrity in cyberspace.

The prevailing concept regarding these rules is "neutral cyberinfrastructure," which the Tallinn Manual defines as "public or private cyberinfrastructure that is located within neutral territory (including civilian cyberinfrastructure owned by a party to the conflict or nationals of that party) or that has the nationality of a neutral State (and is located outside belligerent territory)."[273] The 2020 Oslo Manual defines it similarly.

Analogized to the cyber context, the belligerents are prohibited to conduct hostilities in the form of cyber operations against Neutral's cyberinfrastructure; to conduct cyber operations from within a Neutral's cyberinfrastructure; and, possibly, to abstain from routing cyber operations through a Neutral's territory.

3.3.2 Cyber Operations against a Neutral State

The inviolability of neutral territory entails that neutral cyberinfrastructure is generally protected against any harmful interference or exercise of belligerent rights by the belligerents. Essentially, a belligerent is prohibited from engaging in "the use of network-based capabilities […] to disrupt, deny, degrade, manipulate, or destroy information resident in computers and computer networks, or the computers and networks themselves" of a neutral State. This is also rule 150 of the Tallinn Manual and rule 30 of the Oslo Manual.

Switzerland explicitly addresses this, stating that "in principle, belligerent States are not permitted to damage the data networks of neutral countries when undertaking combat operations via their own computer networks."[274] Similarly, France states that "belligerents must refrain from causing harmful effects to digital infrastructure situated on the territory of a neutral State."[275] Romania does, too, with similar wording.

It is noteworthy that the same protection applies to every cyberinfrastructure located on neutral State ships, aircraft, or diplomatic premises operating outside its territory, all of which fall under the principle of sovereign immunity. This would thus also include systems in outer space (i.e., State satellites). Meanwhile, neutral subjects and neutral property on enemy territory should also be protected from injury. As suggested by the Tallinn Manual's commentary, *Heintschel von Heinegg*, and *Roscini*, it should be so regardless of their character (i.e., private, commercial, or governmental) or the owner's nationality (i.e., neutral or belligerent).

In its commentary to Rule 30, the Oslo Manual also underlines that cyberinfrastructure belonging to a belligerent State located in a neutral State also enjoys neutral protection as long as it is not being abused in support of the military activities of an adversary belligerent State.

The scope of application of the prohibition is also relatively large (i.e., any hostile acts; cf. Article 1 and 2 HC XIII) and thus should cover not only cyber operations amounting to use of force but also those resulting in loss of functionality of cyberinfrastructure. Mere inconvenience, such as temporary website defacement, however, should not. This is backed by the Oslo Manual's commentary on Rule 30. The underlying question is defining the line between the two. *Heintschel von Heinegg* underscores that, in addition to cyberattacks, this prohibition should also comprise any

[272] Switzerland, *supra* note 170.
[273] Tallinn manual 2.0 p. 553, *supra* note 151.
[274] Switzerland, *supra* note 170.
[275] France p. 16, *supra* note 183.

kinetic activities, including physical sabotage, that can negatively impact functionality or make their use impossible.[276] *Roscini*, meanwhile, takes the example of the 2012 Saudi Aramco attack to argue that the language of Article 1 HC V is broad enough to include cyber operations intended to destroy data or software contained in neutral cyberinfrastructure that can lead to widespread disruption.

However, as *Heintschel von Heinegg* argues, mere intrusion (e.g., for cyber espionage purposes) into a neutral's cyberinfrastructure is not covered by this rule. This is also backed by the Tallinn Manual commentary to Rule 92 and the Oslo Manual's commentary to Rule 30. The Oslo Manual states that "(t)he Rule does not apply to espionage. Likewise, it does not apply to the dissemination of propaganda or other activities that are not intended—or are not reasonably expected—to cause death, injury, destruction or damage".[277]

Indeed, during wartime, espionage is not prohibited and is even recognized as permissible between belligerents. Article 24. HC IV explicitly states that "Ruses of war and the employment of measures necessary for obtaining information about the enemy and the country are considered permissible."[278] IHL does regulate some elements of espionage, notably the status of spies as unlawful combatants.[279]

However, this view could potentially evolve. The discussions following the extensive SolarWinds Orion IT and Microsoft Exchange cyber espionage incidents illustrate that States might reconsider their views when faced with practices by other States that they consider out of bounds. One potential avenue for prohibiting cyber espionage against neutral cyberinfrastructure could emerge from the general prohibition of exercising jurisdiction on foreign territory.[280]

Another debated issue among legal scholars is that of (potential) harmful spillover of a cyber operation into a neutral's territory and cyberinfrastructure. According to a strict understanding of the rule—embodied notably in *Roscini*—belligerents should be prohibited from conducting any cyber operations against another belligerent State that have prejudicial incidental effects on neutral territory or infrastructure. In practice, however, this understanding would be somewhat impractical as some spillover is likely due either to the interconnectivity of international networks, the lack of operational control over the spread of such attack, and the *modus operandi* of a cyber operation that could rely on spillover to attain or mask its target.

Thus, Tallinn Manual experts concur that an attack does not violate the law of neutrality if the spillover is not foreseeable. However, if it is, the experts suggest assessing each case on its own merits and balancing between "the right of the belligerents to effectively conduct military operation with the right of the neutral States to remain generally unaffected by the conflict."[281] The Tallinn experts add that "states would be unlikely to regard *de minimis* effects as precluding the prosecution of an otherwise legitimate attack."[282]

This view comes with some open-ended questions. What is foreseeable? How can this be operationalized during the planning phase? What would be the criteria (e.g., geofencing, system-fencing, kill switches)? Would they be publicly disclosed? What would the *de minimis* approach threshold be like in terms of disruption versus inconvenience?

To exemplify the debate over spillover and the threshold for violation further, we can consider two well-known examples: Stuxnet and NotPetya. Both spread beyond their target, but only NotPetya caused non-targeted damage. If the threshold for violation was damage or disruption, an indiscriminate attack similar to NotPetya during an IAC affecting a neutral infrastructure would seemingly be a clear violation of its neutrality and sovereignty. A cyber operation like Stuxnet, which spread in neutral cyberinfrastructure but did not execute its payload due to system fencing, would seemingly not be a violation due to the lack of harm. However, suppose the threshold became mere access to neutral cyberinfrastructure, even without damage and irrespective of whether it was the primary target. In that case, it could be argued that a Stuxnet-type attack would also be a violation of the law of neutrality.

3.3.3 Cyber Operations from Neutral Territory or Infrastructure

State parties to an IAC should generally be prohibited from using neutral cyberinfrastructure or territory to exercise their belligerent rights[283] against other parties. This is particularly highlighted in Tallinn Manual Rule 151 and Oslo Manual Rule 31. This means, for instance, that a belligerent cannot carry out cyber operations associated with the conflict from installations situated on the territory of a neutral State or under the exclusive

[276] Heintschel von Heinegg, *supra* note 29.
[277] Oslo Manual, p. 26, *supra* note 164.
[278] 1907 Hague Convention (IV) respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land, article 24.
[279] ICRC (n.d.). Rule 107. Spies, IHL Database; Beck, N. J. (2011). "Espionage and the Law of War", *American Intelligence Journal,* 29(1), pp. 126-136.
[280] Heintschel von Heinegg, p. 39, *supra* 29.
[281] Tallinn manual 2.0 p. 556, *supra* note 1551.
[282] Ibid.
[283] As Heintschel von Heinegg, *supra note 29*, notes, "it is important to note that the term 'belligerent rights' is not limited to (cyber) attacks but that it refers to all measures a belligerent is entitled to take under the law of armed conflict against the enemy belligerent, enemy nationals or the nationals of neutral States." Such actions comprise detention, requisitions, capture and interception. As such, this prohibition follows from the very object and purpose of the law of neutrality, i.e., to prevent an escalation of the international armed conflict.

control of a neutral State. It also includes the execution of cyber operations by organs and agents of the belligerent State physically located in the territory of the neutral State.[284]

In terms of scope of application, this rule should thus apply to all public and private cyberinfrastructure located on a Neutral's territory (including cyberinfrastructure owned by a belligerent State or its nationals) or under the exclusive control of the neutral State. It also applies extra-territorially to those that enjoy sovereign immunity. France, Italy, Romania, and Switzerland all concur with this view, with France also specifying that a belligerent cannot "take control of computer systems of the neutral State to carry out such operations."[285] There is currently no consensus on whether this prohibition also applies to the use (or abuse) of cyberinfrastructure located outside neutral territory owned by a neutral private corporation or a citizen from a neutral State. Jensen and Walker both argue in favor.

Some authors, such as Jensen, also argue for a broad scope of application: one that includes not only forceful cyber operations but also any harmful actions against another belligerent. *Roscini* concurs, arguing that this would be in line with other rules and doctrines, which do not set any limitations on the type of belligerent action. For instance, Article 49(1) of Additional Protocol I Geneva Convention refers to "all acts of hostilities." Meanwhile, the Hague Convention XIII explicitly provides in its Articles 1 and 2 that belligerents must, respectively, "abstain, in neutral territory or neutral waters, from any act which would, if knowingly permitted by any Power, constitute a violation of neutrality," and that "[a]ny act of hostility is a violation of neutrality and is thus forbidden." Other references are found in the HRAW, HPCR Manual, the German Military Manual, and the UK Manual of the Law of Armed Conflict.[286]

The above documents' references to "acts of hostilities" suggest that cyber espionage could also be prohibited where a neutral State's territory or cyberinfrastructure is concerned, at least when it aims to obtain tactical intelligence regarding the ongoing IAC. Rule 171(b) of the HPCR Manual, which prohibits belligerents from using "neutral territory or airspace as a base of operations—for attack, targeting, or intelligence purposes—against enemy targets in the air, on land, or on water outside that territory," could potentially support this view. However, whether this argument reflects majority opinion is unclear. Furthermore, the extent to which compliance is desirable and feasible is also debatable.

The Oslo Manual and its commentary to Rule 31, however, take a narrow view on the application of this rule, stating that "(i)n light of the interconnected nature of cyberspace (including the Internet), and the degree to which cyberinfrastructure in one country is used in other countries, the Group of Experts considered that it—in view of the current extent of State practice—would be impossible to apply the prohibition reflected in this Rule to cyber operations not constituting attacks."[287] It adds that "(i)n the case of botnets used to conduct attacks, the prohibition relates to the situation in which the botmaster controls a botnet from neutral territory."[288] For activities outside of cyberattacks, the Oslo Manual extends Article 3 HC V to cyber communications installations and argues in Rule 34b that belligerent States are allowed to (and, thus, neutral States must not prevent):

1. Erect a new cyber communication installation[289] on the territory of a neutral State that is exclusively used for non-military communications;
2. Use an existing cyber communication installation established by them before the outbreak of the armed conflict (including for military communications), provided it is open for the service of public messages;
3. Use an existing cyber communication installation established by them before the outbreak of the armed conflict that is not open for the service of public messages, provided it is for non-military communications.

In terms of prohibited techniques, belligerents should also be restricted in their use of spoofing or spear-phishing attacks that leverage a neutral's image, symbol, or name. As pointed out by *Roscini*, cyber operations that "invite the confidence of an adversary with respect to protection" under IHL and betray it, and also result in the death, injury, or capture of the adversary should be considered a prohibited *perfidious act* (Article 37 AP1). That could include, for instance, sending malware attached to an email appearing to be from a neutral

[284] Oslo Manual, p. 27, supra note 164.

[285] Switzerland, *supra* note 170; France, *supra* note 183.

[286] See Article 39 of the Hague Rules of Aerial Warfare provides that '[b]elligerent aircraft are bound to respect the rights of neutral Powers and to abstain within the jurisdiction of a neutral state from the commission of any act which it is the duty of that state to prevent'.; See Rule 166 of the HPCR Manual also states that '[h]ostilities . . . must not be conducted within neutral territory', while Rule 167(a) stresses that belligerents 'are prohibited in neutral territory to conduct any hostile actions'. Rule 171(d) also prohibits the belligerents to conduct '[a]ny other activity involving the use of military force or contributing to the war-fighting effort, including transmission of data or combat search-and-rescue operations in neutral territory'.; The UK Manual of the Law of Armed Conflict declares that '[n]eutral states must refrain from allowing their territory to be used by belligerent states for the purposes of military operations'; Section 1108 of the German Military Manual belligerents are prohibited from conducting 'any act of war' on neutral territory.

[287] Oslo Manual, p. 26, supra note 164.

[288] Ibid. p. 27

[289] I.e. Cyber communication installations may include computers, servers, routers and networks.

State or national, leading to loss of life. However, if the same *modus operandi* was used but did not lead to death, it might nonetheless fall under the prohibitions regarding the misuse of national emblems (Article 39 AP 1).

Additionally, one might consider the protection of images, symbols, and names of neutral humanitarian organizations such as the ICRC. Indeed, according to Article 38(1) AP 1, if a belligerent used their logo for its phishing attacks, they would be in violation of the Geneva Convention[290]. If one applies the same logic to neutral States in cyberspace (both during peace and war), it might be possible to discard the loss of life threshold of a perfidious act, thus drastically lowering the violation threshold.

3.3.4 Cyber Operations through Neutral Territory or Infrastructure

The debate over whether the routing of certain types of data across neutral cyberinfrastructure violates neutrality has been introduced in Section 3.2.3. Legally, it boils down to whether the transport of a "cyber weapon" that falls under Article 2 HC V overrules Article 8 HC V or not. With regards to neutral prevention duty, the debate also included practical concerns around the feasibility of detecting and stopping cyberattacks routed through neutral territory. From the point of view of the belligerent's negative duty, it includes practical concerns about the controllability of the routing path.

Specifically, physical infrastructure usually offers many potential communication paths between two places, while the Border Gateway Protocol that routes the data is based on trust. Hence, it is generally assumed that a belligerent cannot know, control, or plan which route the data packets of its cyber operation will take on its way to its target. This makes it impractical, if not impossible, to ensure that a cyber operation is not routed through an infrastructure located within a neutral's territory.

Still, there are some caveats to the uncontrollability of routing. First, in many remote places, such as islands, cyberattacks that reach them or originate from them will by default always pass through one or several specific countries due to limited access to undersea cables and Internet exchanges where autonomous systems interconnect.

Second, if at least one of the belligerents is surrounded by neutral neighbors, any cyberattack on it will go through neutral territory, even if it may be hard to determine whose. The caveat to the caveat for both the first and second point is that there is also the option of satellite-based Internet.

Third, the path of data can also be controlled if it uses private Internet cables or a next-generation protocol such as SCION, which gives senders and receivers more control over the routing.[291] Given the limited prevalence of SCION, this doesn't change anything today. However, it may be an argument for maintaining that cyber operations through neutral territory are theoretical legal violations of neutrality even if no practical consequences arise from them, as the degree of controllability of routing may change in the coming decades.

Fourth, it is possible to control the route of a human intelligence agent that delivers malware directly onto an enemy's system with a USB stick or something similar.

The majority of the Tallinn experts, Kastenberg, and Kelsey, consider that cyber operations leveraging (complete or incomplete) cyber weapons and malicious code analogous to kinetic weapons, ammunition of war, or war material. If so, such cyber operations would be generally prohibited under Article 2 HC V, which prohibits the transit of munitions of war through neutral territory. Some also see an implicit acknowledgment in the US DoD cyberspace policy report (2011), which mentions "overflight rights." This reversed its initial position in the 1999 US DoD *Assessment of International Legal Issues in Information Operations*. The 2015 US Law of War Manual later re-reversed this 2011 position, arguing that "it would not be prohibited for a belligerent State to route information through cyberinfrastructure in a neutral State that is open for the service of public messages, and that neutral State would have no obligation to forbid such traffic."

Both the American and the French *Opinio Juris*[292] have explicitly referenced Article 8 HC V as an exception to Article 2 HC V. A minority of the Tallinn experts also reject the application of Article 2 to cyberinfrastructure as it was intended to refer to the physical transportation of weapons. France also takes this view, explicitly stating that "routing a cyberattack via the systems of a neutral State without any effect on that State does not breach the law of neutrality, which prohibits only the physical transit of troops or convoys."[293] Another argument is the low risk of escalation and harm (to the neutral) due to simple routing. France and the US explicitly underline that the routing of cyber activities through a neutral State is only permissible under the condition that it must not have any destructive effects within the neutral State.

[290] ICRC (n.d.). *Rule 61. Improper Use of Other Internationally Recognized Emblems*, IHL Database

[291] Perrig, A., Szalachowski, P., Reischuk, R., & Chuat, L. (2017). SCION: A Secure Internet Architecture. scion-architecture.net

[292] US DoD (2016). Law of War manual ; France, *supra* note 183.

[293] France, *supra* note 183.

To a degree, these views resemble Higson's plea for a right or regime of transit in cyberspace that would be synonymous to concepts such as *freedom of navigation* and *peaceful passage* (Article 10 HC XIII; San Remo Rule 20(a)). Higson underlines that the international exchange of data is necessary for the continued functionality of the Internet —the public core of which is increasingly recognized as a common good that needs protection.[294] Higson also makes the comparison between the Internet and the Gibraltar/international straits—i.e., high volume of traffic; overlap of State sovereignty; free and accessible—which grants under the law of the sea a right of transit to belligerents who must, however, refrain from any hostile activities—including electronic surveillance. Such an analogy is, however, far from perfect. Naval navigation routes are still limited with some unescapable bottlenecks such as straits. Meanwhile, warships can be attributed relatively easily, and their sea routes can be detected. In contrast, the routes taken by the data packet in cyberspace are (for now) difficult to control, and their content is not always detectable or attributable.

Switzerland did not take any explicit positions as to the routing questions, possibly to avoid prevention burdens. Its *Opinio Juris* does, however, hint—through omission—that it does not see itself bound to prevent transiting cyber operations on publicly available networks such as the Internet.

3.4 Remedies to Violations

Both neutral and belligerent States can willingly or unwillingly violate their duties. In this case, the injured State has a right to use remedies generally provided under the law of State responsibility to react against internationally wrongful acts. And if the violation amounts to a use of force, by the *jus ad bellum*.[295] The difference is that a violation creates both a right and a duty for the aggrieved neutral State, while it merely creates a right for the aggrieved belligerent State. To note, when remedies are legitimately pursued by the belligerent, neutral States have a general duty to acquiescence and tolerate the enforcement.

As reminded by Heintschel von Heinegg, these remedies generally aim to (1) induce the State at fault to comply with its obligations and (2) allow the aggrieved party to preserve its security interests. In some cases, remedies can also be conducted to induce the provision of reparations.

The scope and range of remedies taken by a belligerent can be varied and cross-domain. They range from non-retaliatory remedies, such as protesting and seeking moral or material reparations, to more retaliatory ones, such as retorsion or countermeasures. Among these, countermeasures and sanctions seem to be the most discussed topics—albeit still marginal compared to peacetime discussions—in academic literature and State views on international cyber law. The remedies are listed and summarized in Table 6.

An aggrieved neutral State's right and duty to remedies can be tied to a belligerent's hostile act against the Neutral (e.g., cyber operation against Neutral territory or cyberinfrastructure) or the non-respect of the Neutral's territorial inviolability (e.g., cyber operation from its territory or cyberinfrastructure). As detailed earlier, harmful spillovers from belligerent cyber operations could also potentially violate neutrality.

An aggrieved belligerent's right to enforce the law of neutrality comes into force if the neutral State fails in its obligations, be it non-participation, prevention, impartiality, or acquiescence. The decision by the injured belligerent to use this right or consent to the Neutral's violation of its duty remains at the discretion of the belligerent.

In the literature, a key example of a violation is when a neutral State is unwilling or unable to comply with its obligation to terminate (or prevent) a violation of its neutrality by the enemy. This case is explicitly laid out in Rule 153 of the Tallinn Manual, which refers to the case as a form of self-help generally accepted by customary international law.

It is also explicitly addressed in US *Opinio Juris* as early as its 1999 assessment, which stated that, in addition to demanding to stop the violation, a belligerent has the "right to use force to neutralize a continuing threat located in the territory of a neutral State, but not acting on its behalf, when the neutral State is unable or unwilling to execute its responsibility to prevent the use of its territory as a base or sanctuary for attacks on another nation."[296] This view was reiterated in its 2011 DoD *cyberspace policy report*. Contentiously, it also argues in favor of such a right to remedies during a NIAC against a "neutral" that is harboring terrorists.

3.4.1 General Requirements

Each remedy has a few general requirements. The most elementary are these: the existence of a violation of the law of neutrality, the calling upon the responsible State to fulfill its obligations, and the cessation of any retaliatory remedy once a violation has ceased.

In addition, according to Article 49 ILC ASR, the retaliatory remedy can only be legitimate if directed "against a State which is responsible for an internationally wrongful act." Some military manuals

[294] See call by the Global Commission on the Stability of Cyberspace for a norm to protect the public core of the Internet.

[295] Roscini, *supra* note 35.

[296] US DoD, *supra* note 261.

also reflect this element (e.g., Ecuador, Canada, US, New Zealand, and Italy).[297]

The use of remedies also requires an internationally wrongful act that is attributable to the responsible State. Without going into the nitty-gritty of the attribution debate,[298] it should be underlined that neither the fact that a cyber operation originates from a neutral State's governmental cyberinfrastructure nor that it has been routed through cyberinfrastructure located in a neutral State is sufficient evidence for attributing the operation to those States. This view is based on the *ICJ's Corfu Channel* case, which claimed that "it cannot be concluded from the mere fact of the control exercised [...] over its territory […] that that State necessarily knew, or ought to have known, of any unlawful act perpetrated therein."[299]

As for the process of attribution itself, the current *Opinio Juris* on the matter seems to crystalize around the opinion that the customary international law of state responsibilities supplies the standards for attributing acts, including cyber activities, to States. These are organs of the State (Article 4) empowered by law to exercise elements of governmental authority (Article 5), acting on the instructions, or under the direction or control, of the State (Article 8) and acknowledgment and adoption of the act as the State's own (Article 11). A State may also incur responsibility for its role in aiding or assisting an internationally wrongful cyber operation by another State (Article 16). Furthermore, the emerging consensus is that there is no obligation to disclose the evidence of such attribution.

Some States, such as the UK and Finland, also underline that there is no duty to disclose the information upon which the attribution is made publicly. Finland also argues that "it may be possible to attribute a hostile cyber operation only afterwards whereas countermeasures normally should be taken while the wrongful act is ongoing."

Finally, the right to retaliatory remedies does not apply to every violation of neutrality. Instead, it applies only if the violation in question harms the legitimate security interest of said belligerent State.[300] That is, **if the belligerent State is "injured" by the violation as understood under Article 42 of the *International Law Commission's Articles on State Responsibility for Internationally Wrongful Acts* (ILC ASR)**. For instance, this would not be the case if a belligerent takes measures against a neutral State's cyberinfrastructure (e.g., a DDoS attack), not implying a military advantage over the enemy. The right to respond to such violation is then exclusively reserved to the neutral State itself.[301] In the latter case, Neutrals have a right to take action to prevent this violation.

3.4.2 Reparations

A common remedy to a violation of the law of neutrality has been explicit protest—for instance, through diplomatic channels—of the violation against its perpetrators and a demand for both the cessation of the violations and some reparations. According to norms of customary international law, any State victim of a violation of international law is entitled to reparations. There exist numerous forms of reparations, including restitution, compensation, or satisfaction.[302] If any physical injuries have resulted from the violation, a victim State can also claim specific damages (i.e., monetary compensations).

In addition to the Articles 37 and 35 ILC ASR, HC IV, and AP 1, there are multiple examples and jurisprudence that illustrate and inform State practice on reparations following a violation of the law of neutrality: the 1937 sinking of the neutral US ship Panay, the 1864 attack on the confederate CSS Florida by the US in a neutral port in Brazil, or the 1944 bombing of Schaffhausen, Switzerland, by the US Army Air Forces. The last incident is particularly illustrative: Following the bombing, the Swiss ambassadors were called in by the US and apologized to. The US Secretary of State issued a statement regretting the affair, and several installments were then paid as damages.[303]

In cyberspace, similar or analogous scenarios are also foreseeable: e.g., a belligerent could mistarget a cyber operation against its enemy and end up disabling instead neutral cyberinfrastructure. This could be due, among other things, to malcoding or technical malfunction (e.g., linked to automation) or simply human error. Consider for instance, a malware initially targeted at a specific enemy system but whose geofencing or systemfencing contingency mechanism triggers in public or private neutral infrastructure (with a similar system to the belligerent) and delivers its payload, causing damage to the system. In this relatively explicit case, the victim State could seek the replacement of the destroyed material, such as hardware, software, or even data—if that is possible. It could also seek compensation—financial or otherwise—for both the actual and future foreseeable physical and financial losses resulting from the damage to servers. Finally, one can also imagine that it could seek assurances or guarantees of non-repetition.[304]

[297] ICRC (n.d.). *Rule 145 Reprisals*
[298] See for instance, Florian Egloff's works
[299] ICJ (1949). *Corfu Channel (United Kingdom v Albania),* p. 18
[300] Roscini, *supra* note 35; Tallinn Manual 2.0 p. 560, *supra* note 151; Heintschel von Heinnegg, *supra* note 29.
[301] Ibid.
[302] ICRC (n.d.). *Rule 150 Reparation*
[303] Downey W. G. (1951). Claims for Reparations and Damages Resulting From Violation of Neutral Rights, *Law and Contemporary Problems*, 16, pp. 487-497
[304] Australia (2019). *Australia Non Paper Case studies on the application of international law in cyberspace*

The amount of damages a State is entitled to has always been a contentious issue. This will probably be similar for the cyber context, especially as calculating damages and costs from cyberattacks is also quite difficult and debatable. Without going into detail, there are currently numerous discrepancies between methods to calculate actual, direct, and indirect costs of cyberattacks. There are also various cost elements to consider, from response time, containment and mitigations cost, hardware and software replacement, profit or functioning loss.

Historically, agreements on reparations have sometimes required the use of arbitration courts to settle for the States. This was notably the case in the *1872 Alabama Arbitration*, whereby the US sought reparations from the UK as the latter had allowed or helped the construction on its territory of a Confederate ship that sunk numerous Union ships during the American Civil War. It remains a key case for the law of neutrality as it set the basis of a Neutral's duty of "due diligence."

As a side note, if we transpose and analogize the Alabama ruling into cyberspace, we can make the following assertions: a (belligerent) victim from an attack conducted by its enemy using (cyber) weapons provided by a neutral could claim reparations. At the same time, this could also indicate that a Neutral's failure—or negligence—to prevent an illegal arms export to one of the belligerents could potentially create an obligation to pay compensation for the damage caused with these arms.[305]

Another interesting case to be considered regarding compensations is the use, destruction, or requisition by a belligerent of neutral property located under a belligerent's jurisdiction (e.g., territory or occupied territory). As previously seen, it is generally considered that neutral property and individuals abroad enjoy the protection provided by their neutral status. However, *jus angary* (cf. Articles 53–54, Regulations respecting the Laws and Customs of War on Land, annexed to the Hague Convention of 1899) provides that the belligerent, under the contingency of military necessity, is allowed to use or destroy railway plants, telegraphs, telephones, or ships that belong to a neutral company or private person.

The requirement is that it provides just compensation for it, which is generally considered complete restitution of the *status quo ante bellum.* If it affects private infrastructure, the *Norwegian claims of 1922*[306] following the US requisition of Norwegian ships indicate that the owners' loss of profit should be compensated based on that of similar owners in the sector.

Thus, despite the views of the Tallinn Manual and scholars that private cyberinfrastructure abroad are protected from belligerent attacks, it would be possible to argue that this exception also applies to cyberspace, either based on the analogy of cyberspace to telegraphs and other ICT mentioned in the articles mentioned above or simply based on military necessity rationales and principles also applying to conflicts leveraging cyberspace.

This would open up the door to many new possible scenarios and questions. For instance, in what specific cases could *angary* be leveraged? What kind of compensations would be adequate for the use of cyberinfrastructure? Following restitution, what guarantee could a belligerent provide that it didn't alter the Neutral's cyberinfrastructure for future use (e.g., installing a backdoor)? Would the use of a requisitioned neutral cyberinfrastructure for launching a cyber operation be permitted? Would it amount to a perfidious act if it is done in secret? Would the owner of the requisitioned party be required to declare it? What would be the risks of escalation?

3.4.3 Retorsion

Retorsion refers to unfriendly acts that do not breach international law and can therefore be adopted at any time. Retorsion can be useful when other remedies are unavailable (e.g., due to proportionality) or are politically ill-suited. Typical examples include declaring individuals *persona non grata*, severing diplomatic relations, withdrawing economic concessions, or breaking trade relations. All of these could potentially be used to respond to a violation in cyberspace. Cyber-specific examples of retorsion might include sending warnings to cyber operatives belonging to another State, observing the adversary's cyber activities on one's network using tools such as "honeypots," or slowing down malicious cyber operations conducted by another State.[307] Others can be found in the European Union's Cyber Diplomacy Toolbox, such as official Statements and demarches by Member States or the EU. Some States, such as the US and Estonia, consider cyber sanctions as retorsions.

However, the extent to which such measures would terminate the violation depends on the case at hand. While it would be hard to see its practical usefulness in the case of a neutral cyberinfrastructure being used by a belligerent to target its enemy, one could always envisage such measures—as a preliminary step of denunciation before further actions—for lesser violations of neutrality, such as the provision of means

[305] This suggestion was advanced by Jan Lemnitzer during his presentation at the 2020 Hague Conference on Cybernorms "Due Diligence in Cyber space: are we heading for a Cyber Alabama?"

[306] Cour Permanente D'arbitrage (1922). Norwegian Shipowners' Claims

[307] Kosseff, J. (2020). "Retorsion as a Response to Ongoing Cyber Operations" in Taťána Jančárková et al (eds), 20/20 Vision: The Next Decade (CCD COE 2020) 17–22.

of warfare (e.g., "cyber munitions" to the enemy) to the enemy.

3.4.4 Countermeasures

Now often confounded or combined with reprisals, **countermeasures[308] are remedies that would violate international law except for the fact that they are proportionate "self-help" measures designed to terminate actions by another State that violate international law—or, in some cases, to secure reparations.** Compared to retorsion, these would, under normal circumstances, be illegal under IL and IHL. In the Tallinn Manual, these are addressed in Rules 20–25. In addition to the general requirements mentioned above, there are at least four other key/specific requirements depending on the case: the seriousness of the violation, the respect of the fundamental principles of IHL, prior notification, and reversibility.

Seriousness of Violation

As per the Tallinn Manual, a criterion for belligerent countermeasures against a neutral unwilling or unable to address a violation of its neutrality is the seriousness of the violation. This goes back to the application of the *de minimis* exception. The commentary also underlines that seriousness must be considered in the context of the IAC and not *in abstracto.* A given example that does not reach the seriousness threshold is that of "establishing the capabilities to hack into the personal email accounts of low-level members of the enemy's armed forces."[309]

This is akin to the current international discussions around countermeasures. Indeed, some States, such as France, explicitly deal with these in their *Opinio Juris* and mention cyber operations with certain consequential negative effects (e.g., military or economic power, security, or survival capacity) as triggering its right to respond.[310]

It is unclear whether this seriousness criterion is widely shared. *Roscini*, for instance, argues that the neutrality violation does not need to be serious to trigger the aggrieved belligerent's right to respond. Given that the majority of States have not expressed their views on this specific issue, it is still unclear which interpretation will take hold in practice.

Additionally, countermeasures by an aggrieved belligerent can only be justified as a countermeasure against the neutral State in the presence of an internationally wrongful act attributable to it.[311] This is clearly expressed in Article 24 of the 1939 *Harvard Draft Convention on the Rights and Duties of Neutral States in Naval and Aerial War*, according to which "[a] belligerent may not resort to acts of reprisal or retaliation against a neutral State except for illegal acts of the latter."[312]

IHL Principles

As recognized by the UN GGE 2015 report, the application of the fundamental IHL principles – i.e., humanity, necessity, proportionality, and distinction – is another requirement for any countermeasure in cyberspace. The operationalization of these principles within the targeting process and legal reviews remains relatively opaque. Apart from a few comments, no State has been transparent in its planning processes and practices.

In their *Opinio Juris*, the UK, Australia, Austria, Estonia, Australia, the US, the UK, Norway, New Zealand, the Netherlands, Germany, and Switzerland have explicitly underlined the respect of the principle of proportionality and/or necessity. Switzerland, among others, has also underlined the respect of IHL norms, *jus cogens,* fundamental human rights, and diplomatic and consular inviolability.

As a general caveat, some States like Israel have highlighted that certain practices that could leverage cyberspace "have never been considered to be attacks as such" and are thus not subject to these IHL targeting principles.[313] This includes, for instance, certain types of electronic warfare, psychological warfare, economic sanctions, seizure of property, and detention.

Prior Notification

Under the law of neutrality, an aggrieved belligerent State is not entitled to resort to countermeasures immediately. The belligerent State must usually first notify the neutral State and allow enough time for remedy. This follows from rule 22 of the San Remo Manual, which states that "if the neutral State fails to terminate the violation of its neutral waters by a belligerent, the opposing belligerent must so notify the neutral State and give that neutral State a reasonable time to terminate the violation by the belligerent."

According to the same article, an exception to this duty does exist. According to *Heintschel von Heinegg,* it is based on Article 168(b) HPCR: "an immediate response by the aggrieved belligerent [without notification] is lawful if (1) the violation constitutes a serious and immediate threat to the belligerent's security, (2) there is no feasible and timely alternative, and (3) the enforcement measure is

[308] See the CCDCOE's cyberlaw toolkit entry for countermeasures for an introduction.
[309] Ibid.
[310] France, *supra* note 183.
[311] Roscini p. 273, *supra* note 35.
[312] (1939). Harvard Draft Convention on the Rights and Duties of Neutral States in Naval and Aerial War, *American Journal of International Law* 33, p. 179.
[313] Schöndorf, R. (2020). *Israel's perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations.* Speech at the US Naval War College's event on "Disruptive Technologies and International Law".

necessary to respond to the threat posed by the violation."[314] The Tallinn Manual corroborates this in its commentary of Rule 153.[315]

Another exception to prior notification is given under Article 52 Para.1(b) and Article 52 Para 2 ILC ASR, which states that an injured State must notify and offer to negotiate with the violator unless "urgent countermeasures are necessary to preserve its rights."[316]

For countermeasures in cyberspace, this derogative view for notification is underlined by, *inter alia*, France, the Netherlands, New Zealand, Italy, Norway, Switzerland, the UK, the US, and Israel as well as the Tallinn Manual 2.0 experts. The Israelis, for instance, state that there is "no absolute duty under international law to notify the responsible State in advance of a cyber countermeasure."[317] Norway justifies this derogation based on the reasoning that providing such notification might reveal sensitive methods or capabilities or prevent the countermeasures from having the necessary effect.

Highlighting the rationale behind this widespread view, France underlines that the "possibility of taking urgent counter-measures is particularly relevant in cyberspace, given the widespread use of concealment procedures and the difficulties of traceability."[318] From a strategic and operational point of view, such a position is understandable. States have little interest in limiting their strategic choices in the domain and would rather push for an exception to eventual additional burdens brought by the law of neutrality.

Reversibility

A last general requirement for countermeasures is reversibility. According to Article 49(3) ILC ASR, they "shall, as far as possible, be taken in such a way as to permit the resumption of performance of the obligations in question."

In practice, reversibility could be transposed in a variety of fashions, depending on the countermeasure. Among other things, one could imagine using a kill switch on a malware disseminated against a belligerent using neutral infrastructure to conduct an attack to stop an ongoing cyber countermeasure once the violation has ceased (i.e., either the neutral has retaken control of its infrastructure, or the responsible belligerent has stopped). Another example would be a cyber operation—similar to ransomware—that encrypts the target's data and releases it once compliance is assured.[319]

Non-forcible Countermeasures

Once the aggrieved party has considered and/or fulfilled all the requirements, it could conduct non-forcible countermeasures.[320] Countermeasures that would amount to the *use of force* against a neutral or belligerent State are illegal according to Article 50 ILC ASR. The latter, which reflects customary international law, provides that countermeasures cannot affect the prohibition of the threat and use of force. Most western States—bar Israel—explicitly refute any use of force for cyber countermeasures. This view is shared, *inter alia*, by the UK, Italy, Norway, Australia, the Netherlands, France, the US, Finland, New Zealand, and Switzerland. The latter stated in its *Opinio Juris* that "countermeasure must not violate certain fundamental substantive obligations such as the prohibition on the use of force."

As reiterated in most available *Opinio Juris*, cyber-related, as well as non-cyber-related breaches of international obligations, may be responded to with cyber and non-cyber countermeasures. Within the cyber environment, countermeasures can take various formats, depending on the creativity, targets, and intention of the injured State. Hence, one could envisage several countermeasures, such as "cyber-demonstration" or a show of force/capabilities to deter wrongdoing. An example could be overtly hacking (e.g., defacement) into the State's cyberinfrastructure.[321] To note, Germany has argued that "a State may – a *maiore ad minus* – engage in cyber reconnaissance measures in order to explore options for countermeasures and assess the potential risk of side effects if such measures fulfill the requirements for countermeasures."[322]

The extent to which these are suitable for answering offensive acts by belligerents on a neutral's territory is debatable. One would envisage them more as a response to a lesser violation. This would also be the case for cyber sanctions, where the right to employ economic sanctions against neutral States supplying or permitting the supply of war material to an enemy belligerent is quite firmly established.

Such non-forcible countermeasures could be used by the aggrieved belligerent to attempt to terminate violations of the law of neutrality that amount to the *use of force* (but not armed attack).[323] Such violations could include, *inter alia*, non-neutral services such as the transfer of arms or military material, the

[314] Heintschel Von Heinneg p.45, *supra* note 29.
[315] Tallinn Manual 2.0 *supra* note 151.
[316] CCDCOE, *supra* note 324.
[317] Schöndorf, *supra* note 313
[318] France p. 8, *supra* note 183.
[319] Lynch, J. (2018). *Why reversible cyberattacks could become standard in digital warfare*. Fifth Domain.
[320] These are measures that would otherwise be contrary to the international obligations of an injured State vis-à-vis the responsible State, if they were not taken by the former in response to an internationally wrongful act by the latter in order to procure cessation and reparation.
[321] The strategic and operational rational behind these would need to be assessed in details as there is a clear risk of losing one's strategic advantage by revealing its presence.
[322] Germany, *supra* note 343.
[323] Roscini p. 274, *supra* note 35.

recruitment of corps de combatants, or even specific commercial or network access discrimination.[324]

Collective Countermeasures

Another unresolved and controversial issue is the question of collective countermeasures. Article 48(1) ILC ASR states that a non-injured State can appeal to the responsibility of a State that commits an internationally wrongful act if "the obligation breached is owed to a group of States including that State, and is established for the protection of a collective interest of the group" (e.g., breach of a multilateral treaty) or "the obligation breached is owed to the international community as a whole" (e.g., aggression, genocide, and self-determination).[325] The ILC left open the question as to whether States other than the injured one may respond, in addition to invoking responsibility, with countermeasures.

Estonia was the first country to explicitly note in its 2019 legal opinion that a State can conduct cyber countermeasures on behalf of, or in collaboration with, a State facing unlawful cyber operations. Estonia went even further than the ILC did. It explicitly stated that the right for collective countermeasures in response to cyber operations is not limited by the two cases mentioned above. Collective cyber countermeasures are also NATO's preferred view. New Zealand has tepidly supported it in its legal opinion: "Given the collective interest in the observance of international law in cyberspace, and the potential asymmetry between malicious and victim States, New Zealand is open to the proposition that victim States, in limited circumstances, may request assistance from other States in applying proportionate countermeasures to induce compliance by the State acting in breach of international law."[326] However, most States have not addressed it. France explicitly rejects it.

Whether collective countermeasures would be conceivable and lawful in the case of a violation of the law of neutrality remains to be debated. The underlying rationale behind Estonia's endorsement could resonate with both neutral and belligerent States who may lack the capacity, expertise, and capability to deal with hostile cyber operations conducted against them. It can be assumed that an injured State would prefer to have the possibility to deter potential violations but also to respond to them more effectively.[327]

3.4.5 Forceful or Armed Response

Still contentious, the use of force as a remedy to a violation of neutrality is also legal under certain conditions or legal interpretations: *forceful enforcement of a party's duty* and *forcible countermeasures*.

Use of Force by the Neutral

According to the law of neutrality, a neutral State must terminate a violation of its neutrality by force, if necessary. This is clearly implied in Article 10 HC V, which states, "The fact of a neutral Power resisting, even by force, attempts to violate its neutrality cannot be regarded as a hostile act." This is similarly phrased in Article 48 of the Hague Rules of Aerial Warfare and rule 168(b) and 169 HPCR Manual.

However, the UN Charter has superseded the Hague Convention's regarding the legality of the use of force. Thus, the exceptions laid out in Article 2(4) UNC—i.e., self-defense and Chapter VII—apply in this case. Accordingly, in the course of their prevention duty, neutral States will be allowed to use kinetic or cyber force "only if such violation amounts to an armed attack or the forcible reaction is authorized by the UN Security Council."[328]

This is re-iterated in the latest Oslo Manual, whose commentary on Rule 30 states that "(i)n case of an abuse by a Belligerent State of objects or infrastructure located in neutral territory, cyber operations against the Neutral State amounting to use of force under the Charter of the United Nations Article 2(4) will be lawful only if they are consistent with the inherent right to self-defense (as recognized by Article 51 of the Charter) or when authorized by the Security Council."[329]

Thus, this obligation to use force, if necessary, against a (cyber or physical) violation of neutrality is still effectively in place. Indeed, as has been observed by Bothe, "the Charter of the United Nations grants a right to use counter-force; the law of neutrality may, under certain circumstances, impose an obligation to exercise this right."[330]

Historically, while some use led to war with the belligerent, others have become customary and have not led to war. A notable example is the Swiss strictly defending their airspace during WW2 by shooting down Allied and Axis planes and interning their pilots.

Use of Force by the Belligerent

Similarly, a belligerent State could use force in two scenarios: in reaction to an armed violation by the neutral State and in reaction to a neutral State's failure (or unwillingness) to uphold its duty of prevention.

Regarding the former, the requirement for a forceful response is that the neutral's violation amounts to an *armed attack* against the injured belligerent. If the violation falls short of an *armed attack*, the belligerent

[324] Ibid.
[325] Schmitt, M. (2019). *Estonia Speaks Outs on Key Rules for Cyberspace*. Just Security
[326] New Zealand, p. 4, *supra* note 235.
[327] Schmitt, *supra* note 325.
[328] Roscini, p. 274, *supra* note 35.
[329] Oslo manual, p. 26, *supra* note 164.
[330] Bothe, p. 561, *supra* note 28.

would not be allowed to use forcible countermeasures as they are unlawful under the *jus ad bellum* regime.

Despite this unlawfulness, some scholars have argued for a right to forceful countermeasures. As argued by *Schmitt*, this view mostly relies on the reading of the separate opinion of Judge Simma in the ICJ's 1996 *Oil Platforms case,*[331] which is considered, by some, to endorse forceful countermeasures.[332] Transposed to cyberspace, the opinion's approach would, according to Schmitt, "permit countermeasures crossing the use of force level, but not that of an armed attack, in response to unlawful cyber operations of the same severity."[333]

This view has its critics, notably Hataway, which counter-argues that the separate opinion "simply makes the commonsense observation that "a State may of course defend itself" even against uses of force that do not amount to an armed attack, but such defense is subject to limits of "necessity, proportionality, and immediacy in a particular strict way."[334]

Regarding the latter, the law of neutrality generally allows an injured belligerent to take necessary and proportional action to terminate a violation of a neutral's territory by another belligerent if the neutral is unable or unwilling to do so himself. Under certain conditions, this could include the *use of force* or *armed attack*.

This is clearly re-stated in rule 22 of the San Remo Manual, which states that: "If the violation of the neutrality of the State by the belligerent constitutes a serious and immediate threat to the security of the opposing belligerent and the violation is not terminated, then that belligerent may, in the absence of any feasible and timely alternative, use such force as is strictly necessary to respond to the threat posed by the violation."[335]

That view, somewhat controversially, is supported by several States. For instance, the UK Military Manual states that "[i]f a neutral State is unable or unwilling to prevent the use of its territory for the purposes of military operations, a belligerent State may become entitled to use force in self-defence against enemy forces operating from the territory of that neutral State: this, however, 'will depend on the ordinary rules of the jus ad bellum.'"[336]

Applying this to the cyber context, *Roscini* surmises that "an armed reaction, therefore, only would be allowed if it is the aggressor State that uses the territory of the neutral State, including the cyberinfrastructure located therein, to conduct kinetic or cyber hostilities against the victim of the armed attack, and the forcible reaction on neutral territory is necessary and proportionate to repel the armed attack; or if the reaction has been authorized by the Security Council."[337]

Kastenberg similarly argued that "if a neutral State cannot or does not take action to halt a cyber-attack, a belligerent may choose to counter by physically attacking the neutral State's communications infrastructure."[338]

The US was even more explicit in its 1999 DoD Cyberspace policy report, stating that: it has the "right to use force to neutralize a continuing threat located in the territory of a neutral State, but not acting on its behalf, when the neutral State is unable or unwilling to execute its responsibility to prevent the use of its territory as a base or sanctuary for attacks on another nation."[339]

[331] ICJ (2003). *Oils Platforms (Islamic Republic of Iran v. United States of America).*

[332] Hathaway, O. (2014). "The Drawbacks and Dangers of Active Defense" in Pascal Brangetto et al (eds), Proceedings (CCD COE 2014), p. 39-50.

[333] Schmitt, M. (2019). *France's Major Statement on International Law and Cyber: An Assessment*. Just Security

[334] Ibid.

[335] San Remo Manual (1994)

[336] UK (2014). Joint service manual of the Law of Armed Conflict, section 1.43

[337] Roscini p. 274-275, *supra* note 35.

[338] Kastenberger p. 56, *supra* note 129.

[339] US DoD p.16, *supra* note 261.

Type of Remedies	Requirements	Examples
General (applies to all types of remedies)	• Previous violation of the law of neutrality by a belligerent or neutral State • Violation can be legally attributed to a party • Aggrieved State is "injured" (Article 42 ILC ASR) • Aggrieved State has called upon the responsible State to fulfill its obligations • Must be suspended once the violation has stopped • Target is the State responsible for the violation	
Reparations	• Proportional to the violation	• *Satisfaction*: Official excuses, expression of regret, • *Restitution*: Of seized (cyber) infrastructure • *Compensation*: Financial or material reparations • Investigating and charging responsible individuals
Retorsion	• Unfriendly acts that can be adopted at any time	• Declaring diplomats or hackers *persona non grata* • Ending diplomatic relations • (Cyber) sanctions • Sending warnings to cyber operatives belonging to another State • Slowing down malicious cyber operations conducted by other States • Public attribution of a cyber operation
Countermeasures	• General requirements • Violation needs to be serious enough* • Aim is to induce an adversary to comply, not retaliation • Preceded by an unsatisfied demand for reparation or compliance with the violated international law* • Prior notification (with exceptions) • Proportional to the violation • Decision at the highest level of government • Respect fundamental IHL principles, ordinary rules of *Jus ad Bellum*, peremptory norms (*jus cogens*), and the obligation to respect diplomatic and consular inviolability • The violation must represent an immediate threat to security, and there is no other feasible and timely alternative • The enforcement measure taken is strictly necessary to respond to the threat posed by the violation • Reversibility	• Nondestructive cyber operations could be launched to shut down networks or systems that another state is using for a cyberattack • Suspension of treaty • Seizure of property • Show of (cyber) force
Use of Force*	• General and countermeasures requirements* • The violation must amount to armed attack*	• Kinetic attack or destructive cyber operation against a neutral's cyberinfrastructure

*Table 6: Summary of remedies to violations of the law of neutrality and their requirements. Requirements marked by an * are still debated.*

4 Challenges and Developments

Historically, the law of neutrality has been a useful instrument to both belligerent and neutral States to avoid or mitigate escalation during emerging or ongoing conflicts. In the current context characterized by a return of great power competition, the assertion of cyberspace as a future domain of warfare, and the increasing societal and economic dependence on and interdependence of ICT, it is only legitimate to wonder and explore if the law of neutrality could still serve its principal function in cyberspace.

As illustrated throughout the previous section, however, the application of the law of neutrality to cyberspace still faces many challenges, including legal imprecision, overlapping or contradicting use of analogies, and analytical hurdles. In this section, we take a step back and discuss the broader challenges and opportunities for the development and practical application of the law of neutrality in cyberspace. We discuss the limitations and challenges linked to the scope of application of the law of neutrality as well as its reliance on territorial sovereignty before addressing eventual practical challenges to impartiality. We then take stock of the current state of the *Opinio Juris* and State practice before highlighting a few political and legal hurdles to the further development of the law of neutrality. We then make a case for the continuing relevance of the law before opening up the discussion on the potential application of neutrality to foreign policy in the context of cyber operations.

4.1 Scope of Application

The scope of application and relevance of the law of neutrality in cyberspace is constrained in several ways: the type of conflicts, the type of actors, and the type of activities.

4.1.1 International Armed Conflict

The most **direct limitation to the application of the law of neutrality in cyberspace is that it requires an acknowledged international armed conflict (IAC)**. However, the great majority of hostilities between rival States occurring in or leveraging cyberspace are not linked to any IAC. Rather, they occur under the threshold of war in the so-called "grey zone," where IHL does not *de facto* apply. Hence, the law of neutrality would apply only in a relatively limited number of cases.

There are two important caveats. First, some States, most notably the US, state in their *Opinio Juris* that they will apply IHL principles in their cyber operations even if they occur under this threshold. This could potentially include or be extended to neutrality principles. Second, NATO has recently communicated that in its view, cyberattacks can also cumulatively reach the threshold of an armed attack.[340] This is a change that might open up new questions and discussions as to the required threshold for the application of the law of neutrality and potentially make the law of neutrality apply to a set of under-the-threshold cyber operations.

Aside from the required threshold for its application, there are also unresolved questions about **when the law of neutrality stops applying in cyberspace.** The law of neutrality traditionally ceases to apply when the conflict in question ends, which, in practice, should entail a certain degree of normalization of relations and a lack of hostilities. However, in the cases of conflicts within cyberspace, the lack or cessation of hostilities might be difficult to gauge and monitor, at least for unsophisticated or purely disruptive cyber operations. These latter ones are already legion in peacetime and form the backbone of low-intensity conflicts.

4.1.2 Non-International Armed Conflict

If one considers the requirement for an IAC as being the principal limitation of the law of neutrality, one could argue that the law of neutrality can—or should—provide at least some guidance, if not apply, during certain nontraditional conflicts. Indeed, the last decades' shifting conflict landscape—including increased transnational threats, internal wars, and non-State actors—has reanimated discussions about and support for neutrality rules in non-international armed conflicts (NIACs).

Scholars like Jensen argue in favor of these rules by highlighting the potential benefits of equalizing the legal playing field across State and non-State actors. Neutrals would enjoy reinforced legal protections and States could use the additional legal rights to enforce their sovereignty. Succinctly, he proposes promoting a doctrine of neutrality for non-State actors through unilateral State declarations.

Other scholars, such as Melzer, argue that the pragmatism of neutrality's core principle—i.e., prevention duty—has already found its way into NAICs and, thus, could potentially extend to cyber conflicts. He notably references the *OAS Convention* (1929*), the Protocol on Duties and Rights of States in the Event of Civil Strife* (1957), and the *International Committee of the Red Cross (ICRC) Official Statement* (2001*)*. The following is stated in the latter: "It is the ICRC's view that it [the Fifth Hague Convention] can also be applied by analogy in situations of non-international conflicts, in which combatants either from the government side or

[340] NATO. (2021). *Brussels Summit Communiqué*. nato.int. Article 32

from armed opposition groups have fled into a neutral State."[341]

Melzer further argues that the practical consequences of non-State belligerents abusing "neutral"[342] territory to conduct (cyber)attacks against other States are similar to those foreseen in traditional neutrality law—most notably, the loss of the neutral territory's inviolability and, as such, the possibility for remedies. Notable real-world examples include *Al-Qaida's* attacks against the United States from within Afghanistan, *Hezbollah's* attacks against Israel from within Lebanon, and the attacks of the Revolutionary Armed Forces of Colombia (*Fuerzas Armadas Revolucionarias de Colombia,* or FARC) against Colombia from within Ecuador. In all these cases, the aggrieved States have conducted extraterritorial military interventions directly against the respective groups under the justification that their "neutral" host States were either unable or unwilling to protect the attacked State's interests within their territory, reasoning that strongly resembles that of permissible remedies against a neutral's violation of its prevention duty.

Transposed to cyberspace, this could point towards the potential legality of countermeasures or self-defense against non-State actors (e.g., terrorists or rebels with sophisticated cyber capabilities) that conduct *armed* cyber operations from cyberinfrastructure found within the territorial remit of a *de facto* "neutral" State. This could also apply to those cyber operations that take place within an established NIAC (i.e., of sufficient extent, duration, or intensity). Thus, if one follows Germany's and the Tallinn Manual's position, this would mean that singular, lower-intensity but large-scale cyber operations, "such as a large-scale intrusion into foreign cyber systems, significant data theft, the blocking of internet services and the defacing of governmental channels or websites will usually not singularly and in themselves bring about a non-international armed conflict."[343]

Only a limited number of States have already addressed this issue, with some diverging opinions. Regarding remedies, the US, in its 1999 DoD report, stated that "[a]ttacks on insurgents or on terrorists and other criminals using a neutral nation's territory as a refuge may also be justified when the neutral State is unable to satisfy its obligations."[344]

Regarding self-defense, meanwhile, Germany generally accepts that self-defense measures can target an attributed non-State actor.[345] France, however, does not recognize the extension of the right to self-defense to acts perpetrated by non-State actors without the attribution to a State. However, France does make an exception for non-State actors that are "quasi-States," such as ISIS. Moreover, it recognizes that the general practice may shift toward accepting the right to self-defense against non-State actors.[346]

If *Opinio Juris* and State practice crystalize around this view, it would be reasonable to expect such self-defense operations (kinetic or cyber) to follow established requirements under international law. Specifically, they should be directed only at the responsible non-State actor, the aim is to induce it to stop its attack, they are temporary and reversible, and they respect fundamental human rights.[347] Additionally, and as explicitly stated by Germany, the non-State actor and the State in question are to respect IHL principles.[348]

In addition, the use of force by the aggrieved State should be—in the case of an armed attack—permissible, but it would have to meet the conditions of necessity and proportionality. While this has been explicitly acknowledged in the *Opinio Juris* of France, the Netherlands, and the US, it would normally reflect customary international law—i.e., the *Nicaragua Opinion*—and as such, it is a line of thought probably shared by most States. A small caveat needs to be highlighted: the US views on the right to self-defense are somewhat unique. It contends that the right exists in the advent of any unlawful use of force, thereby rejecting the existence of a threshold of armed attack distinct from the threshold of the use of force.[349]

Coming back to the justification for these self-defense measures, these are often framed within the context of the recognized basic obligation of States to prevent hostile activities against other States from within their territory (i.e., due diligence duty or principle of non-intervention) rather than neutrality. However, in cyberspace, the transposition of this duty/obligation of due diligence remains debated. Nonetheless, these discussions rejoin those laid out in the prevention duty section, notably around actual versus constructive knowledge or minimum capabilities.

4.1.3 Actors

As a legacy of its codification context, **the law of neutrality focuses nearly exclusively on States and**

[341] ICRC (2001). "International Committee of the Red Cross Official Statement of 8 March 2001 to the United Nations High Commissioner for Refugees Global Consultations on International Protection"

[342] To be noted, they cannot be considered as neutral in a legal sense as there is no state of IAC. The literature often speak of "third party" in the case of NIACs.

[343] Germany, (2021). On the Application of International Law in Cyberspace p. 7 ; Tallinn Manual 2.0, p. 83, *supra* note 122

[344] US DoD, p. 22, *supra* note 261.

[345] Deutscher Bundestag (2015). Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Dr. Alexander S. Neu, Andrej Hunko, Wolfgang Gehrcke, weiterer Abgeordneter und der Fraktion Die Linke, BT-Drs. 18/6989, p. 11

[346] France pp. 8-9, *supra* note 183.

[347] Roguski, *supra* note 180.

[348] Germany p. 7, *supra* note 357: "Germany holds the view that cyber operations of a non-international character, e.g. of armed groups against a State, which reach a sufficient extent, duration, or intensity (as opposed to acts of limited impact) may be considered a non-international armed conflict and thereby also trigger the application of IHL."

[349] Roguski, *supra* note 180.

attributed State-linked actors. This is a narrow focus, considering the plurality of actors, non-governmental actors' roles, and the difficulties linked to legally receivable attribution prevalent in cyberspace.[350] Indeed, the few provisions, such as those for individuals joining *corps of combatants* working for a belligerent, which could apply to cyberspace are not that relevant in practice. Unfortunately, the domain's reality is that non-State actors seemingly conduct most cyber operations, often with blurred, hard-to-prove, or non-definitive affiliations with State institutions. While this practice allows some degree of plausible deniability for States engaging in cyber operations, it limits the regulative, deterrent, and de-escalatory benefits from applying the law of neutrality.

Similarly, **the law of neutrality does not directly regulate the behavior of private firms or private individuals.** They are relatively free to trade with the warring belligerents, at least as long as they do it impartially and respect export controls.[351] This is another challenge in the law of neutrality's application, especially when considering the prevalence of private and individual activities and ownership in cyberspace. (see Section 4.3.2).

4.1.4 Types of Cyber Operations

The law of neutrality's scope does not apply to a good portion of State-sponsored cyber operations (i.e., political/economic cyber espionage or cyber-enabled influence operations). The operational ambiguity of the intent behind such operations can blur the lines between cyber operations covered by the law of neutrality and those that aren't, eventually or potentially allowing States to dismiss accusations of neutrality violations.

Linked to that last point, the law of neutrality's focus on transgression by physical acts, such as the provision of personnel and arms to belligerents, does not fit well with certain cyberspace activities' intangibility, which might be harder to detect and, thus, prevent. Indeed, the growth of non-tangible means of support (e.g., supplying data, imagery, or 3D printing designs for producing digital or physical arms) provides neutral States with a far greater range of options to violate their non-participation duties.[352] Uncertainty regarding these intangible and dual-use technologies risks undermining the whole premise and core purpose (i.e., preventing escalation) upon which the law of neutrality was built. As such, this would, admittedly, only reinforce a trend since WW2, whereby neutral States have regularly not complied with their obligations under the law of neutrality (e.g., Iraq). They either openly or clandestinely assisted one party to an international armed conflict to the other belligerent's detriment.

4.2 Territorial Sovereignty

The law of neutrality is closely linked to the concept of territorial sovereignty. Article 1 HC V states, "The territory of neutral Powers is inviolable." All other rules in HC V are derived from this principle. As discussed in Section 3.1.1, there is also a broad agreement amongst States that territorial sovereignty applies to cyberspace. However, three major issues must be considered concerning computer networks. First, cyberspace is a cross-domain environment. All objects belonging to it are physically located within land, water, airspace, or outer space, in each of which there is a different conception of sovereignty. Second, sovereign States cannot reasonably be expected to control all data coming to, from, or through their territory. Third, even though territorial sovereignty would imply exclusive jurisdiction over data hosted in a neutral country, there may be other claims for lawful access that could force companies to hand them over to a belligerent.

4.2.1 Cross-cutting Domain

There is a widespread acceptance of framing cyberspace as a functional domain with its own operational logic. However, cyberspace as a cross-cutting domain is different from territorial domains in that an object is never exclusively part of it. Every electron, photon, computer chip, cable, or antenna is physically located within land, water, air, or outer space. The strictness of the law of neutrality varies between these domains; hence, cyber activities can be regulated differently in international law based on their location. The regimes for outer space and international waters are two special cases of particular interest.

Outer Space

Given its global posture, a large part of US Military communications goes through spaceborne systems. Switzerland highlights in its legal opinion that territorial sovereignty does not apply to outer space, and hence, territorial neutrality does not apply. Thus, according to this premise, a belligerent military satellite flying 350 kilometers above Switzerland that is used to communicate with belligerent forces would not constitute a violation of neutrality since it is not in Switzerland's territory. However, sovereignty and neutrality can still apply based on exclusive state control over an object in space. The key question is whether or not the access and impartiality rules for the telegraph, the telephone, and the radiotelegraph networks (Article 8 and 9 HC V) can also be applied to satellite

[350] To note, nowadays, technical attribution is more often than not relatively feasible. Legally receivable attribution, however, less so.

[351] With the risk of becoming a target of course.

[352] Nasu, *supra* note 40.

constellations and even to individual satellites that communicate through radio waves with ground stations (Section 4.3.2). This is further complicated because satellites are often operated by commercial providers or by international consortia involving several countries. On the one hand, Schmitt argues that in general, "individual states do not avoid responsibility by virtue of multinational ownership".[353] On the other hand, it is unclear whether or not this also applies to a small stake in a project. Switzerland's involvement in the French remote sensing system "Composante Spatiale Optique" provides an interesting model for addressing neutrality concerns in a multinational collaboration. It boils down to two factors. First, the share of the Swiss participation in the system's total costs may not be significant. Second, a suspension clause must ensure that Switzerland can interrupt its participation in and payments for the project at any time if they would undermine its neutrality.[354]

International Waters

Submarine cables transport well over 95 percent of international data traffic. However, as Kraska notes, the international law on submarine cables in international waters (Section 2.2.1) remains very murky, and "(i)n the meantime, States may expect that adversaries' plans to disrupt international submarine cables during naval warfare are limited only by their national laws and their imagination."[355] As such, it might be advisable for neutral countries to strengthen their legal arguments and act as norm entrepreneurs in favor of stronger protection of these cables in times of war as part of a neutral public core of the Internet (Section 4.3.3). However, history also cautions that powerful States may ignore such norms if it gives them a clear military advantage.

4.2.2 Degree of Control

As highlighted in Section 2.3, States should not be expected to exert the same degree of control over the Internet as over previous technologies due to dependence on private companies, the volume of data exchange, and the logic of the standards for the transport and network layers of the Internet. This point is also stressed by Switzerland's legal opinion, which underlines that cyberspace is less controllable than airspace, where neutral duties are based on means at disposal and are not as absolute as on land.

Consequently, it can be argued that it would be impractical to have a duty to prevent attacks through neutral territory based on constructive knowledge, even if the attack is equivalent to the use of kinetic force. Regarding a prevention duty of attacks from neutral territory, we would argue that it should be in accordance with the *means at disposal* of the State, whether it occurs in sovereign waters, airspace, or land.

4.2.3 Lawful Access

States are principally allowed to engage in intelligence activities. However, as discussed in Section 3.2.2, sharing military intelligence about a belligerent to another belligerent violates neutrality. For example, in the First World War, Switzerland tried and convicted two high-ranking officers for sharing intelligence with Germany and decrypting Russian telegrams on behalf of it.[356] Whereas these individuals engaged in a very blatant violation of professional secrecy and neutrality, there is currently a debate in many countries about negligent violations of professional secrecy.

Some countries have domestic laws that force companies to hand over data accessible to them worldwide (i.e., in the context of crimes and intelligence activities). Regarding the former, the Budapest Convention on Cybercrime encourages mutual assistance. However, somewhat controversially, Section 103 of the *Clarifying Lawful Overseas Use of Data (CLOUD) Act* also gives US law enforcement a clear basis to demand overseas data from its tech giants unilaterally in the context of serious crimes and terrorism. Regarding the latter, the Chinese 2017 *National Intelligence Law,* the American Section 702 of *the Foreign Intelligence Surveillance Act* (FISA), and the American *Executive Order 12333* are examples of wide-ranging surveillance permissions. As argued by the European Court of Justice in its Schrems II judgment,[357] standard contractual clauses are not necessarily sufficient to justify a transfer of data to a country without adequate legal data protection. Companies may have to carry out transfer risk assessments to comply with European data protection laws.

By using similar logic, it can be argued that governments could violate neutrality through the negligent sharing of military intelligence with a belligerent. This would imply a neutral duty to use data protection best practices in accordance with its means for sensitive data, particularly intelligence collected on

[353] Schmitt, M. (2006). International Law and Military Operations in Space. Max Planck Yearbook of United Nations Law Online, 10(1), 89-125. p. 107

[354] Schweizerischer Bundesrat. (2020). *Botschaft zur Genehmigung der Rahmenvereinbarung zwischen der Schweiz und Frankreich über die bilaterale Kooperation zur Nutzung des Satellitensystems «Composante Spatiale Optique» und zum entsprechenden Verpflichtungskredit.* fedlex.admin.ch pp. 9917&9918

[355] Kraska, J. (2020). *Submarine Cables in the Law of Naval Warfare.* lawfareblog.com

[356] Steiner, S. (2014). Oberstenaffäre. In U. Daniel, P. Gatrell, O. Janz, H. Jones, J. Keene, A. Kramer & B. Nasson (Eds.) *International Encyclopedia of the First World War*.

[357] European Court of Justice. (2020). Decision C-311/18 on international transfers of personal data from the EEA.

belligerents. For example, consider the use of strong encryption with local key management or local storage when relying on hardware, software, and cloud services from tech companies of a belligerent.

In the case of Switzerland, this issue may not just be relevant for the military and the intelligence service but also to organizations that are not legally concerned with neutrality. The ICRC regularly collects data about belligerents as part of its humanitarian mission. Furthermore, the Society for Worldwide Interbank Financial Telecommunications (SWIFT) has one of only four data centers in Switzerland. It is the only center that stores both European zone and Trans-Atlantic zone messages.

4.3 Impartiality

As discussed in Section 2.1.3, the impartiality duty of Neutrals can be curtailed by the UN Security Council sanctions. However, it is not just international law that limits neutral impartiality. First, technological complexity makes it difficult for small States to have cutting-edge (defense) technology and not create procurement and maintenance dependencies on larger States. Second, the fact that private companies are allowed to export war material to belligerents under the law of neutrality can be at odds with the impartiality function/duty of neutrality and a source of friction. Third, globalization and network effects have created private global governance institutions that can de facto mandate unequal restrictions on belligerents.

4.3.1 Technological Complexity

Neutrality needs to be credible. Hence, many States argue that neutrality needs to be armed, including with up-to-date technology. However, as modern weapons systems have become more complex, smaller States like Switzerland or Sweden cannot domestically produce all their military technology. The suppliers of high-tech defense systems may use this dependence to influence the Neutral's security policies. Nilson and Wyss call this the "armed neutrality paradox" and specifically highlight the development of Sweden and Switzerland after the Second World War.[358] With regard to Switzerland, the US achieved full informal participation in the strategic embargo against the Eastern bloc, the Coordinating Committee for Multilateral Export Control, based on economic threats as well as the export of modern defense technology.

Ever since the founding of the Federal Telegraph Workshop in 1851, Switzerland has had a domestic industry for ICT hardware, which has also supplied its armed forces. Key companies have included Hasler AG, which emerged from the Federal Telegraph Workshop, Autophon AG, and Zellweger AG. These merged into Ascom AG when Switzerland liberalized its market for telecommunications hardware in the 1990s. However, Ascom still lost most of its market share. Today, it's very clear that the Swiss economy, as well as to some degree its armed forces, must rely on foreign technology procurement and sometimes even maintenance. This spans from computer chips to 5G networks to fighter jets.

4.3.2 Private Exports to Belligerents

As discussed in Section 3.2.2, neutral States are not obliged to restrict private exports of war material to belligerents (Article 7 HC V; Article 7 HC XIII). Hence, there are only a few limitations on private exports. First, neutral States may impose export restrictions, as long as they are imposed impartially on all belligerents (Article 9 HC V). There are national and international export control regimes for cryptography, as well offensive or weaponizable dual-use software. However, these do not yet cover many technologies, and the phrasing of international agreements, such as the Wassenaar Arrangement, remains relatively vague. Second, general due-diligence obligations still apply and could force host countries to terminate direct participation in cyber operations provided as a service. Third, if one of the three analogies to previous technologies holds, neutral countries may need to ensure that private infrastructure services would, in principle, be offered impartially to both belligerents (Article 8 and 9 HC V).

The Swiss delegation to the Hague Conference was surprised that private war material exports to belligerents had not been deemed a violation of neutrality.[359] Indeed, it is easy to see how private trade with belligerents can conflict with the goal of avoiding escalation, and there are many examples of belligerents taking unfriendly measures to suppress private arms exports to their opponent from nonbelligerent as well as neutral countries. For example, in the First World War, Switzerland foiled German plans to blow up a Neuchâtel munitions factory supplying France.[360] In more recent times, Russia's military intelligence service GRU has allegedly engaged in sabotage and poisoning operations against weapons manufacturers in Czechia and Bulgaria

[358] Nilsson, M., & Wyss, M. (2016). The Armed Neutrality Paradox: Sweden and Switzerland in US Cold War Armaments Policy. *Journal of Contemporary History, 51*(2), pp. 335-363.

[359] Before the international codification of neutral duties and rights in The Hague, Switzerland had imposed such a neutral duty on itself in domestic law. Schweizerischer Bundesrat (1870). *Verordnung betreffend Handhabung der Neutralität der Schweiz*. fedlex.admin.ch; Schlussbericht der schweizerischen Delegation. (1907). pp. 102 & 103

[360] Vuilleumier, C. (2019). The Swiss Police Forces and Counter-Intelligence (1914–1918). In J. Campion, L. Lopez & G. Payen (Eds.) *European Police Forces and Law Enforcement in the First World War*. p. 189.

that supplied the Ukrainian army;[361] and, in 2021, Israel may have conducted a sabotage operation against an Iranian drone manufacturer that has provisioned Hamas.[362] In a cybersecurity context, private exports to belligerents refer not only to goods but also to services. This is illustrated by the role of US companies in the 2008 Russian-Georgian war (Section 3.2.4), which may have undermined the US neutrality toward the conflict.

Particularly for permanently neutral States, such considerations strengthen the case for export controls that prohibit private exports of war material and specific services to belligerents in an international armed conflict, even if this would not be necessary according to the Hague Conventions.

Satellites

Satellites may be a particularly contentious point with regards to impartiality and private exports. Article 8 HC V's authorization of the use of neutral communications infrastructure extends to the transmission of information of military significance. As such, belligerents may use neutral satellite networks to communicate if they are made available impartially to all belligerents. However, the provision of remote sensing imagery used for target acquisition may be considered by belligerents as an act of active involvement regardless of impartiality. Article 47 of the drafted 1923 *Hague Rules of Aerial Warfare* states that "A neutral State is bound to take such steps as the means at its disposal permit to prevent within its jurisdiction aerial observation of the movements, operations or defenses of one belligerent, with the intention of informing the other belligerent." The use of the word jurisdiction rather than territory and the fact that in 1923, "aerial observation" was understood to apply to a space that extends outwards indefinitely, would indicate that neutrals could have a duty to ensure that a company registered in their country does not sell military-relevant remote sensing data to a belligerent.

Yet, even if this prevention duty is rejected, it is important to highlight that a neutral satellite may still qualify as a lawful military target.[363] In its 1999 *DoD Assessment*, the United States distinguished between relaying information through satellites and satellites as information-generating systems. The provision of the latter, which includes satellite imagery, weather data, and navigation systems, to a belligerent may give the opposing belligerent the right to take proportional acts in self-defense.[364] In terms of state practice, in the 1991 Gulf War the United States delayed the release of commercial Landsat imagery to US news media and France denied Iraq access to commercial satellite imagery from its SPOT satellites, as this could have revealed the position of US troops.[365] Further, in 2004, the EU and the US signed an agreement "to prevent hostile use of satellite-based navigation and timing services, while simultaneously preserving services outside areas of hostilities."[366]

4.3.3 Private Global Governance

The global governance, development, and maintenance of cyberspace is decentralized and involves multiple types of stakeholders. Whereas Russia and China would prefer an intergovernmental model of governance, many Western and like-minded States support multistakeholderism based on the premise that it furthers innovation, growth, and freedom of expression. However, this also means that there are a few private institutions outside of a neutral's territory that could theoretically restrict its ability to remain impartial.

ICANN

The Internet Corporation for Assigned Names and Numbers (ICANN) is a private nonprofit organization headquartered in California. ICANN assigns IP-address blocks and top-level domains in the domain name system (e.g., .com, .ch). Originally, the organization received this Internet Assigned Numbers Authority (IANA) function as a US Department of Commerce contract. However, since October 1, 2016, the nonprofit has been entirely independent. ICANN is now governed by a multistakeholder community, including many technical representatives. Governments can only participate in an advisory function.

Still, China in particular fears that in an armed conflict, the US could order ICANN or VeriSign, the US-based operator of the primary root server of the domain name system, to restrict Chinese access to them and, more importantly, to shut down or reassign its top-level domains to the outside world.[367] It must be noted that ICANN has internal rules for assigning top-level domains and that US courts and the US government have argued against using US jurisdiction over ICANN for political ends.[368] Still, hypothetically, ICANN could decide on or

[361] Bellingcat. (2021). How GRU Sabotage and Assassination Operations in Czechia and Bulgaria Sought to Undermine Ukraine. bellingcat.com

[362] Wintour, P. (2021). Blast at Iranian complex housing drone factory injures nine. theguardian.com

[363] Heintschel von Heinegg, W. (2017). Neutrality and Outer Space. In *International Law Studies, 93*, p. 541.

[364] Office of the General Counsel. (1999). *An Assessment of International Legal Issues in Information Operations.* pp. 9-10.

[365] Baker, John, & Dana Johnson. (2001). Security Implications of Commercial Satellite Imagery. In John Baker, Kevin O'Connell, & Ray Williamson (Eds.) *Commercial Observation Satellites: At the Leading Edge of Global Transparency*. (Santa Monica, CA: Rand). p. 104

[366] Agreement on the Promotion, Provision and Use of Galileo and GPS Satellite-based Navigation Systems and Related Applications. Article 11.2.

[367] Binxing, F. (2018). *Cyberspace Sovereignty*. Springer: Singapore. pp. 326 & 327.

[368] United States Court of Appeals for the District of Columbia. (2015). Susan Weinstein, et al., Plaintiffs-Appellants, v. Islamic Republic of Iran, et al., Defendants-Appellees, Internet Corporation for Assigned

be forced to create a de facto restriction of public networks in neutral countries that is not impartial between belligerents.

SWIFT

SWIFT is a cooperative society with headquarters in Belgium. SWIFT connects more than 10,000 financial institutions and handles about 80% of global payment messaging. A decision by SWIFT to disconnect banks of a belligerent from its network can significantly increase the difficulty and cost of engaging in trade with it. From March 2012 to 2015, based on EU sanctions, and again in November 2018, based on pressure by the US, SWIFT disconnected the Central Bank of Iran and several other Iranian banks from its network. This de facto forced many companies in countries without sanctions to observe US sanctions. SWIFT is a closed, privately-owned computer network; however, network effects and the resulting dependence of global finance and global trade on SWIFT means that it could de facto mandate economic sanctions for neutral countries in an armed conflict. Moreover, if Article 9 HC V were to be judged applicable to SWIFT by analogy, it could be argued that a decision to remove the banks of one belligerent could also legally violate the neutrality of the host country of the organization (Belgium), if not that of all countries with significant infrastructure on their territory (US, Netherlands, Switzerland).

A Neutral Public Core?

Assuming that there is no political support for a more intergovernmental approach to computer network governance, there may still be a solution that would defuse some concerns about dependence on private global governance institutions. Specifically, the Netherlands Scientific Council for Government Policy has proposed a norm to designate the Internet's public core as a global public good that should be protected from unwarranted State interference.[369] Elements that have been suggested as belonging to this public core are certain standards (TCP/IP), physical infrastructures (DNS servers, undersea cables), and organizations (internet exchanges, CERTs).[370]

Designating certain aspects, such as DNS servers, as neutral would define them as illegitimate targets for belligerents while also prohibiting their weaponization against a belligerent. The specific norm of having CERTs as "digital first responders" that neither attack others nor are allowed to be the target of an attack might be the one with the most existing support. The UN GGE consensus report in 2015 already stated in Article 13k, *"States should not conduct or knowingly support activity to harm the information systems of the authorized emergency response teams (sometimes known as computer emergency response teams or cybersecurity incident response teams) of another State. A State should not use authorized emergency response teams to engage in malicious international activity."*[371]

4.4 Opinio Juris and State Practice

The law of neutrality in cyberspace has room for development. States and scholars are still at the beginning of a long conversation concerning the legal and practical applications of IHL to cyberspace. Currently, there is still little available *Opinio Juris* and even less State practice on neutrality in cyberspace. Despite the general stabilizing benefits that IHL can bring, this might change slowly, as States have practical and political disincentives to create new burdens on themselves voluntarily.

4.4.1 Opinio Juris

The US, the Netherlands, Switzerland, Italy, Romania, and France are the only States that have explicitly addressed the law of neutrality in cyberspace in their legal opinions. It is thus hard to argue there is a consensus within the international community regarding the applicability and application of the law of neutrality to cyberspace. This is especially true as some States are still reluctant to recognize the general applicability of IHL, of which the law of neutrality is part.

Despite the lack of consensus, these six views and the anecdotal references by other States are valuable for two reasons. First, they put neutrality in the foreground of international legal discussions, which could induce other States to address and develop it. The same is true for the Tallinn and Oslo Manuals and the small body of academic scholarship that addresses, explores, and comments on neutrality in cyberspace through analogies, case studies, and scenarios. Second, the existing legal opinions make it possible to discern a nexus of core issues, rights, and duties (see Table 7), all of which have been discussed in Section 3.

Unfortunately, the legal opinions only contain limited guidance towards the operationalization of these neutrality rules. Those with the most capacity or interest in them will likely shape this process further (i.e., cyber and/or great powers and permanent neutral States). Historically, this has generally been the case, whereby the main driving forces behind the law of

Names and Numbers, Appellee-Garnishee. Brief for the United States as Amicus Curiae.

[369] Broeders, D. (2015). *The public core of the Internet: An International Agenda for Internet Governance*. Amsterdam, Netherlands: Amsterdam University Press.

[370] Broeders, D. (2017) Aligning the international protection of 'the public core of the internet' with state sovereignty and national security. *Journal of Cyber Policy, 2*(3), 366-376. p. 368

[371] UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. (2015). A/70/174. un.org. p.8

neutrality have either been neutrals trying to ascertain or justify their rights or privileges and great powers

Topics/ Countries	US	Netherlands	France	Switzerland	Italy	Romania
Scope of Application			X			X
Sovereign Right of Neutrals	(X)			X		
Non-participation/ Abstention Duty	(X)	X		X		
Impartiality Duty	X	X			X	
Prevention Duty	X	X	X	X		
Acquiescence Duty	(X)					
Cyber Operations against Neutral Territory or Infrastructure	(X)		X	X		X
Cyber Operations through Neutral Territory or Infrastructure	X		X			
Cyber Operations from Neutral Territory or Infrastructure		X	X	X	X	X
Remedies for Violation of Neutrality	X					

Table 7: Summary of State Opinio Juris addressing various neutrality subjects. Note: "X" denotes an explicit reference, "(X)" an implicit one. See Annex D for corresponding quotes.

accommodating them, depending on their current geostrategic interests.

This still seems to be true. With its strong legalistic tradition and early cyber power, the US seized the issue of neutrality in cyberspace as early as 1999 and now addresses most of the core issues delineated earlier. Among permanent Neutrals, only Switzerland, Japan, and Finland have released their views on international cyber law. However, only the Swiss address neutrality in cyberspace, covering many core issues but, interestingly, omitting views on the routing question (incl. the Article 8 exception) and impartiality.

Compared to the cyber powers France and the US, Switzerland's views tend towards a narrower interpretation of neutral duties. An example is the prevention duty. Indeed, while most States having addressed neutrality generally agree that a neutral should prevent that its territory and/or cyberinfrastructures are used by a belligerent, Switzerland only explicitly refers to closed military State systems under its exclusive control. However, whether this is intentional or/and the full scope of their views is debatable. France's position, meanwhile, is more maximalist, underlining that "(t)he neutral State must prevent any use by belligerent States of ICT infrastructure situated on its territory."[372]

4.4.2 State Practice

Historically, the law of neutrality developed largely through State practice unfolding with historical events that prompted states to adopt specific positions to protect their interests. Thus, the development and operationalization of the law of neutrality in cyberspace also rests on developing some degree of State practice on top of *Opinio Juris*.

[372] France, p. 16, *supra* note 183.

While there is general agreement that international law, humanitarian law, and, to some extent, the law of neutrality apply to cyberspace, there is little transparency as to actual State practice applying the law of neutrality to cyber operations. There have been close to no explicit communications by States on how they intend to conduct legal reviews for their cyber operations. This contrasts to kinetic operations, whose legal reviews are more accessible and sometimes public and generally include respecting the law of neutrality.

This absence of State practice is linked to the limited set of existing cases where the law of neutrality could have applied or has been considered to apply in relation to cyberspace. Indeed, no State has ever publicly claimed a belligerent violated its neutrality with its cyber operation. In retrospect, however, one could argue that the law of neutrality could or should have applied during recent IAC, such as the 2020 Nagorno-Karabakh war between Armenia and Azerbaijan, which had cyberwarfare elements.[373] Under this assumption, in-depth case analyses could potentially provide some new insights on State practice.

The case most often mentioned in academic literature is that of the Russian-Georgian war of 2008. However, there is no public legal reasoning on the issue by the US, Russia, or Georgia, and the scholarly legal assessment remains somewhat inconclusive. In short, *Korns* and *Kastenberg* argued that the US, having allowed the hosting of the Georgian Foreign Ministry on its territory (by American firms), had violated (or "endangered") its neutrality by failing to halt military communication between a US host and Georgia (Article 3 HC V) and the creation of a corps de combatant (i.e., US technicians helping keep up the Georgian servers) on US territory. Added to this, the US's impartiality was also put into question as it openly supported Georgia. They also argue that Georgia violated US neutrality by moving assets and data to California servers.

These are points which *Higson* countered by arguing that the law of neutrality didn't necessarily apply in that case as the cyber operations conducted against the Georgian ministry of foreign affairs were not necessarily linked to the armed conflict in question; they were conducted before the start of the hostilities by a criminal network with non-definitive affiliation or attribution. Furthermore, he stipulates that the US didn't fail to uphold its prevention duty due to the telegraph exception, which allows public communication on open networks such as the Internet.

4.5 Looking Forward

4.5.1 International Consensus Building

With the successful conclusion of the OEWG and the discussion of a work program, there is international interest in addressing and developing legal and normative frameworks for cyberspace. The current efforts are mostly geared towards addressing cyber operations under the threshold of war. In practice, this means that the focus has been on developing a set of voluntary, nonbinding norms based on accountability instead of international laws based on responsibilities and duties.[374] Indeed, as reflected and stated in several documents, such as the 2019 *Joint Statement on Advancing Responsible State Behavior in Cyberspace*,[375] States are to be held accountable for violation of the framework of responsible State behavior in cyberspace.

The academic sector and civil society[376] have engaged with the specific issue of neutrality in cyberspace a bit more than governments. However, overall, it remains relatively niche in the greater international cyber law debates as cyberattacks occurring outside of armed conflicts are a more imminent challenge. Having said that, the OEWG and UN GGE discussions might provide a window of opportunity to further discuss, develop, and transpose the law of neutrality to cyberspace. Maybe even more importantly, the advancement of related issue areas could also help to inform the issue of cyber neutrality and be beneficial to its development in the long term. This notably includes **questions around the due diligence obligation, the threshold of use of force, countermeasures, and cyber sanctions.**

The law of neutrality has always been a very slow-moving field. Its codification was slow and occurred after centuries of State practice. Furthermore, it has not seen consequential developments beyond the reaffirmation of its applicability after the Second World War and the adoption of the UN Charter. As such, a new treaty updating the law of neutrality is highly unlikely. As *Kelsey* indicated, one would expect a slow and gradual evolution of norms, customs, code of conduct, and rules of engagement before further codification. Hence, the question of whether there is **progress towards an international consensus on how to operationalize the "musty" law of neutrality in cyberspace is largely contingent on progress in the interlinked discussions**

[373] Mercer, W., Rascagneres, P. & Ventura, V. (2020). PoetRAT: Malware targeting public and private sector in Azerbaijan evolves. Talos Intelligence blog.

[374] See Roguski P. (2020). *Norm-based accountability vs. law-based responsibility for cyber operations.* Presentation at the 2020 Hague Conference on Cyber Norms.

[375] The following countries are included: Australia, Belgium, Canada, Colombia, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Hungary, Iceland, Italy, Japan, Latvia, Lithuania, the Netherlands, New Zealand, Norway, Poland, the Republic of Korea, Romania, Slovakia, Slovenia, Spain, Sweden, the United Kingdom, and the United States of America. See US DoS. (2019). Joint Statement on Advancing Responsible State Behavior in Cyberspace.

[376] The Former Swiss Ambassador Dahinden published an ICT4Peace policy brief on neutrality in the context of cyberspace. See Dahinden, M. (2021). Schweizer Neutralität im Zeitalter der Cyberkregsführung. ICT4Peace

on international cyberlaw, generally and international humanitarian law specifically.

Two factors weigh against the rapid development of the law of neutrality in cyberspace. One is that states might fear the additional burden or operational limitation that could entail. The other is a general weariness or uncertainty of many (non-western) States to address international law in general and, even less so, the law of neutrality.

An example of the former is the debate around the due diligence duty, which—while generally accepted as a customary principle—several States do not consider applying in a binding fashion to cyberspace. The US is, allegedly, hesitant to support a stand-alone due diligence duty because most tech companies are headquartered in the US. In practice, this ambivalence has led due diligence to be relegated to an unclear and undefined norm in the 2015 UN GGE report, as well as being completely dropped from the final draft of the OEWG report.

An example of the latter is the lack of non-western public *Opinio Juris*—bar Iran's—or the relatively little commentary on IL some have provided during the OEWG drafting procedure.

4.5.2 Neutrality for Cyberspace

Whereas applying the law of *neutrality in cyberspace* is this report's focus, neutrality is also a foreign and security policy instrument (Section 1.5) that goes beyond legal rights and obligations. As such, permanently neutral countries may also leverage *neutrality for cyberspace* as part of foreign and security policy. Specifically, neutrality's traditional solidarity function (Section 1.2) might prove useful in future international tensions over cyberattacks and a gridlocked development of international cyberlaw.

More specifically, solidarity means that permanent Neutrals provide good offices and other actionable preventive diplomacy initiatives contingent on their neutral reputations and expertise as bridge builders and mediators. The following is a non-comprehensive list of potential preventive diplomacy initiatives whereby political neutrality as perceived by other parties might play a facilitating role:

First, permanent Neutrals could be particularly suited to facilitating dialogue. This could be at the track 1 or track 2 diplomacy level and include non-State actors. Examples include the Geneva Dialogue on Responsible Behavior in Cyberspace, which brought together many leading companies from the industry, and the Biden-Putin Summit in Geneva, which has been framed as a potential "cyber-détente."[377]

Second, permanent Neutrals could ensure communication and diplomatic relations between parties without direct, official means of communication.[378]

Third, permanent Neutrals could provide forensic analysis services.[379] The financial support of fact-finding activities fits well in the tradition of good offices. For example, Spiez Laboratory has provided neutral expertise in several contentious fact-finding missions related to chemical threats. Similarly, permanent Neutrals could also support initiatives such as the Forum for Incident Response and Security Teams (FIRST), which helps to strengthen CERT cooperation and works to protect the public core of the Internet.

Fourth, permanent Neutrals could support capacity building in other countries, including their legal capacity.

Lastly, permanent Neutrals could provide a safe haven for data from international organizations that enjoy legal immunity. However, this function may be constrained by limited technological autonomy.

[377] Kurbalija, J. (2021). *What is the future of a cyber detente after Biden and Putin's Geneva summit?* diplomacy.edu

[378] Stolz, M. "On Neutrality and Cyber Defence." Proceedings of the 18th European Conference on Cyber Warfare and Security, Academic Conferences and Publishing International, 2019, pp. 56–57.

[379] Mäder, L. (2019). *Wenn der feindliche Zugang zum Computer gleich mitgeliefert wird*. nzz.ch

5 Conclusion

To conclude, a few elements are worth highlighting. First, **there is some — albeit slow — movement in the legal and policy debates around neutrality in cyberspace**. This is worth the attention of policymakers and practitioners, as the law of neutrality could in the future entail practical, strategic, policy, and operational conundrums. While concrete discussions are still in their infancy, both academia and States have started to consider or address the issue. As described in this report, they do so mostly by exploratively analogizing and applying the core rights and duties to cyberspace. Varying and competing opinions have even emerged. This particularly pertains to the "routing question" and its corollary requirements for neutral States to prevent the routing of cyber operations through their territory.

These early discussions highlight several interesting and potentially contentious issues, which will require some clarification through case law, *Opinio Juris*, or State practice. These include, for example, the legality and practicality of governmental CERT cooperation (e.g., with NATO), the export of dual-use software by either the State or private companies, or the necessary knowledge requirements (actual or constructive) to trigger a neutral State's prevention duty.

Despite these rich but niche legal discussions, only four States have addressed the law of neutrality to some extent in their *Opinio Juris*: The US, the Netherlands, France, Italy, Romania, and Switzerland. It is thus difficult to argue that there is any consensus within the international community regarding the law of neutrality in cyberspace. It is also too early to predict the direction these rules will take or which rules States will address in practice.

The extent to which the law of neutrality will see further development remains uncertain due to underlying political disincentives, legal limitations, and practical challenges to its relevance in current contexts. This includes its scope of applicability, which is limited to international armed conflicts and State actors, while most confrontations in cyberspace nowadays not only happen under the threshold of armed conflicts but also involve a diverse set of actors, including private and non-State actors. In addition, the often-ambiguous nature and attribution of cyber operations, most of which apply to espionage, also makes the application of the law of neutrality difficult.

In the context of cyberspace, the law of neutrality's reliance on domain-specific territorial sovereignty also creates additional challenges. Notably, **cyberspace as an artificial domain is also a cross-domain environment whose infrastructure is physically located within land, water, airspace, or outer space, each of which has a different conception of sovereignty and legal specificities according to the law of neutrality**. This traditional attachment to territorial sovereignty also poses some practical challenges for States, notably around the questions—and potential expectations—of the degree of control and access to outgoing and transiting data from one's territory.

The interconnected, privatized, and decentralized nature of cyberspace and its infrastructure and governance might also make the application of central tenets of neutrality arduous, such as the impartiality duty and the fostering of a credible neutral posture. Technological complexity makes it difficult for small States to have the cutting-edge (defense) technology necessary to defend and enforce their neutrality without creating procurement and maintenance dependencies on third States. The same applies to the export of war materials by private companies which, while technically allowed under thelaw of neutrality, can undermine neutral postures. Impartiality could also be challenged by private global governance institutions (e.g., SWIFT or ICANN) that could *de facto* mandate unequal restrictions on belligerents.

Still, the law of neutrality is not an immutable body of law. It has been adapted (at least in practice) to changing historical and technological realities, indicating that this could also be possible in cyberspace. This is particularly so, as several elements and functions of the law of neutrality could remain useful for cyberspace. For example, **the *inviolability of a neutral State's sovereignty* and the *non-participation duty* of a neutral State could provide the neutral with a clear and established legal framework to deter indiscriminate spillover or attacks against its cyberinfrastructure in an armed conflict and to demand reparations in case of violations**. Important open questions revolve around attribution, the role of hacker groups, and forms of intangible support. The *prevention duty* of neutral States could also provide a useful framework for clarifying expected and acceptable behavior to avoid escalation. The basic tenets of this framework are starting to emerge in State *Opinio Juris*, which will likely serve as building blocks for future additions. At the lowest common denominator of the law of neutrality, there is a duty to prevent the belligerent use of military cyber-infrastructure under a neutral State's control. The specifics are still being debated and include the extension to private ICT, the prevention of cyber operations transiting through neutral infrastructure, the type of required knowledge, and the expected required capabilities as well as their burden. Some modalities of *prevention*, *impartiality*, and *non-participation* duties legitimize and protect undisturbed international e-commerce. Meanwhile, military and dual-use technology trade may have to be addressed in national or international export control regimes to guarantee neutral parties' prevention, impartiality, and non-participation obligations.

In the short term, some advancement—or at least clarifications around basic rights and duties—can

be expected as States continue to publish their *Opinio Juris* on international cyberlaw and vow to clarify IHL in cyberspace. However, one must also consider the extent to which non-binding norms—instead of hard binding law—are a more adequate instrument and regulative framework for cyberspace. In the longer term, the evolving debate around cyberspace neutrality will most likely depend on geopolitics, technology, catalyzing events, great powers' interests, and States deciding whether or not to pursue neutrality. As has been the case historically, neutrality might also become topical as conflicts become more cyber-centric and destructive for third-party States**.**

A second, more general conclusion is that one must potentially consider the greater practical and political implications and applications of the legal duties. Additionally, neutral States will become more involved in legal debates and ensure they have the capacity and expertise to do so. Indeed, while there is moderate pressure to prepare research and arguments to operationalize neutrality in cyberspace further, the cyber component in diplomatic crises and armed conflicts is constantly growing. This makes it a potentially interesting and relevant topic for the future. As such, many States should have an interest in reducing the legal uncertainty. The future work program of the OEWG might be a good place to engage further in this debate.

Meanwhile, permanently neutral States might also be interested in thinking about the role of cyber neutrality in their larger digital foreign policy, as well as peace and security policy. For Switzerland, this could include questions of Internet governance and the role of "International Geneva," in addition to opportunities for leveraging the solidarity functions of neutrality in cyberspace to contribute to stability in this space. As discussed above, this could include preventive diplomacy actions and measures, such as cyber-tuned good offices. It might also include a set of actions that more directly engage with the private sector, such as developing channels and collaborative frameworks for the implementation of neutral duties.

Finally, it is important to once more recall that neutrality has historically been "a flexible instrument for safeguarding interests."[380] As such, we should not only seek wisdom in old texts but also ask how cyberspace is different from the earlier communication technologies for which these texts were originally written and what new concepts might make sense as a result. As discussed in this report, one possible answer to the globalized governance of key technical aspects of the Internet by mostly private actors might be to extend neutrality to them.

[380] Schweizerischer Bundesrat. (1993). Bericht zur Neutralität: Anhang zum Bericht über die Aussenpolitik der Schweiz in den 90er Jahren vom 29. November 1993. p.3

6 Annexes

A. Convention (V) Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land

Chapter I: The Rights and Duties of Neutral Powers
Art. 1. The territory of neutral Powers is inviolable.

Art. 2. Belligerents are forbidden to move troops or convoys of either munitions of war or supplies across the territory of a neutral Power.

Art. 3. Belligerents are likewise forbidden to: (a) Erect on the territory of a neutral Power a wireless telegraphy station or other apparatus for the purpose of communicating with belligerent forces on land or sea;
(b) Use any installation of this kind established by them before the war on the territory of a neutral Power for purely military purposes, and which has not been opened for the service of public messages.

Art. 4. Corps of combatants cannot be formed nor recruiting agencies opened on the territory of a neutral Power to assist the belligerents.

Art. 5. A neutral Power must not allow any of the acts referred to in Articles 2 to 4 to occur on its territory. It is not called upon to punish acts in violation of its neutrality unless the said acts have been committed on its own territory.

Art. 6. The responsibility of a neutral Power is not engaged by the fact of persons crossing the frontier separately to offer their services to one of the belligerents.

Art. 7. A neutral Power is not called upon to prevent the export or transport, on behalf of one or other of the belligerents, of arms, munitions of war, or, in general, of anything which can be of use to an army or a fleet.

Art. 8. A neutral Power is not called upon to forbid or restrict the use on behalf of the belligerents of telegraph or telephone cables or of wireless telegraphy apparatus belonging to it or to companies or private individuals.

Art. 9. Every measure of restriction or prohibition taken by a neutral Power in regard to the matters referred to in Articles 7 and 8 must be impartially applied by it to both belligerents. A neutral Power must see to the same obligation being observed by companies or private individuals owning telegraph or telephone cables or wireless telegraphy apparatus.

Art. 10. The fact of a neutral Power resisting, even by force, attempts to violate its neutrality cannot be regarded as a hostile act.

Chapter II: Belligerents Interned and Wounded Tended in Neutral Territory
Art. 11. A neutral Power which receives on its territory troops belonging to the belligerent armies shall intern them, as far as possible, at a distance from the theatre of war. It may keep them in camps and even confine them in fortresses or in places set apart for this purpose. It shall decide whether officers can be left at liberty on giving their parole not to leave the neutral territory without permission.

Art. 12. In the absence of a special convention to the contrary, the neutral Power shall supply the interned with the food, clothing, and relief required by humanity. At the conclusion of peace the expenses caused by the internment shall be made good.

Art. 13. A neutral Power which receives escaped prisoners of war shall leave them at liberty. If it allows them to remain in its territory it may assign them a place of residence. The same rule applies to prisoners of war brought by troops taking refuge in the territory of a neutral Power.

Art. 14. A neutral Power may authorize the passage over its territory of the sick and wounded belonging to the belligerent armies, on condition that the trains bringing them shall carry neither personnel nor war material. In such a case, the neutral Power is bound to take whatever measures of safety and control are necessary for the purpose. The sick or wounded brought under the these conditions into neutral territory by one of the belligerents, and belonging to the hostile party, must be guarded by the neutral Power so as to ensure their not taking part again in the military operations. The same duty shall devolve on the neutral State with regard to wounded or sick of the other army who may be committed to its care.

Art. 15. The Geneva Convention applies to sick and wounded interned in neutral territory.

Chapter III: Neutral Persons
Art. 16. The nationals of a State which is not taking part in the war are considered as neutrals.

Art. 17 A neutral cannot avail himself of his neutrality

(a) If he commits hostile acts against a belligerent;

(b) If he commits acts in favor of a belligerent, particularly if he voluntarily enlists in the ranks of the armed force of one of the parties. In such a case, the neutral shall not be more severly treated by the

belligerent as against whom he has abandoned his neutrality than a national of the other belligerent State could be for the same act.

Art. 18. The following acts shall not be considered as committed in favour of one belligerent in the sense of Article 17, letter (b):

(a) Supplies furnished or loans made to one of the belligerents, provided that the person who furnishes the supplies or who makes the loans lives neither in the territory of the other party nor in the territory occupied by him, and that the supplies do not come from these territories;

(b) Services rendered in matters of police or civil administration.

Chapter IV Railway Material

Art. 19. Railway material coming from the territory of neutral Powers, whether it be the property of the said Powers or of companies or private persons, and recognizable as such, shall not be requisitioned or utilized by a belligerent except where and to the extent that it is absolutely necessary. It shall be sent back as soon possible to the country of origin. A neutral Power may likewise, in case of necessity, retain and utilize to an equal extent material coming from the territory of the belligerent Power. Compensation shall be paid by one Party or the other in proportion to the material used, and to the period of usage.

Chapter V: Final Provisions

Art. 20. The provisions of the present Convention do not apply except between Contracting Powers and then only if all the belligerents are Parties to the Convention.

Art. 21. The present Convention shall be ratified as soon as possible. The ratifications shall be deposited at The Hague. The first deposit of ratifications shall be recorded in a ' procès-verbal ' signed by the representatives of the Powers which take part therein and by the Netherlands Minister for Foreign Affairs. The subsequent deposits of ratifications shall be made by means of a written notification, addressed to the Netherlands Government and accompanied by the instrument of ratification. A duly certified copy of the ' procès-verbal ' relative to the first deposit of ratifications, of the notifications mentioned in the preceding paragraph, and of the instruments of ratification shall be immediately sent by the Netherlands Government, through the diplomatic channel, to the Powers invited to the Second Peace Conference as well as to the other Powers which have adhered to the Convention. In the cases contemplated in the Preceding paragraph, the said Government shall at the same time inform them of the date on which it received the notification.

Art. 22. Non-Signatory Powers may adhere to the present Convention. The Power which desires to adhere notifies its intention in writing to the Netherlands Government, forwarding to it the act of adhesion, which shall be deposited in the archives of the said Government. This Government shall immediately forward to all the other Powers a duly certified copy of the notification as well as of the act of adhesion, mentioning the date on which it received the notification.

Art. 23. The present Convention shall come into force, in the case of the Powers, which were a Party to the first deposit of ratifications, sixty days after the date of the ' procès-verbal ' of this deposit, and, in the case of the Powers which ratify subsequently or which adhere, sixty days after the notification of their ratification or of their adhesion has been received by the Netherlands Government.

Art. 24. In the event of one of the Contracting Powers wishing to denounce the present Convention, the denunciation shall be notified in writing to the Netherlands Government, which shall immediately communicate a duly certified copy of the notification to all the other Powers, informing them at the same time of the date on which it was received. The denunciation shall only have effect in regard to the notifying Power, and one year after the notification has reached the Netherlands Government.

Art. 25. A register kept by the Netherlands Ministry of Foreign Affairs shall give the date of the deposit of ratifications made in virtue of Article 21, paragraphs 3 and 4, as well as the date on which the notifications of adhesion (Article 22, paragraph 2) or of denunciation (Article 24, paragraph I) have been received. Each Contracting Power is entitled to have access to this register and to be supplied with duly certified extracts from it.

B. Convention (XIII) Concerning the Rights and Duties of Neutral Powers in Naval War

Art. 1. Belligerents are bound to respect the sovereign rights of neutral Powers and to abstain, in neutral territory or neutral waters, from any act which would, if knowingly permitted by any Power, constitute a violation of neutrality.

Art. 2. Any act of hostility, including capture and the exercise of the right of search, committed by belligerent war-ships in the territorial waters of a neutral Power, constitutes a violation of neutrality and is strictly forbidden.

Art. 3. When a ship has been captured in the territorial waters of a neutral Power, this Power must employ, if the prize is still within its jurisdiction, the means at its disposal to release the prize with its officers and crew, and to intern the prize crew. If the prize is not in the jurisdiction of the neutral Power, the captor Government, on the demand of that Power, must liberate the prize with its officers and crew.

Art. 4. A prize court cannot be set up by a belligerent on neutral territory or on a vessel in neutral waters.

Art. 5. Belligerents are forbidden to use neutral ports and waters as a base of naval operations against their adversaries, and in particular to erect wireless telegraphy stations or any apparatus for the purpose of communicating with the belligerent forces on land or sea.

Art. 6. The supply, in any manner, directly or indirectly, by a neutral Power to a belligerent Power, of war-ships, ammunition, or war material of any kind whatever, is forbidden.

Art. 7. A neutral Power is not bound to prevent the export or transit, for the use of either belligerent, of arms, ammunition, or, in general, of anything which could be of use to an army or fleet.

Art. 8. A neutral Government is bound to employ the means at its disposal to prevent the fitting out or arming of any vessel within its jurisdiction which it has reason to believe is intended to cruise, or engage in hostile operations, against a Power with which that Government is at peace. It is also bound to display the same vigilance to prevent the departure from its jurisdiction of any vessel intended to cruise, or engage in hostile operations, which had been adapted entirely or partly within the said jurisdiction for use in war.

Art. 9. A neutral Power must apply impartially to the two belligerents the conditions, restrictions, or prohibitions made by it in regard to the admission into its ports, roadsteads, or territorial waters, of belligerent war-ships or of their prizes. Nevertheless, a neutral Power may forbid a belligerent vessel which has failed to conform to the orders and regulations made by it, or which has violated neutrality, to enter its ports or roadsteads.

Art. 10. The neutrality of a Power is not affected by the mere passage through its territorial waters of war-ships or prizes belonging to belligerents.

Art. 11. A neutral Power may allow belligerent war-ships to employ its licensed pilots.

Art. 12. In the absence of special provisions to the contrary in the legislation of a neutral Power, belligerent war-ships are not permitted to remain in the ports, roadsteads, or territorial waters of the said Power for more than twenty-four hours, except in the cases covered by the present Convention.

Art. 13. If a Power which has been informed of the outbreak of hostilities learns that a belligerent war-ship is in one of its ports or roadsteads, or in its territorial waters, it must notify the said ship to depart within twenty-four hours or within the time prescribed by local regulations.

Art. 14. A belligerent war-ship may not prolong its stay in a neutral port beyond the permissible time except on account of damage or stress of weather. It must depart as soon as the cause of the delay is at an end. The regulations as to the question of the length of time which these vessels may remain in neutral ports, roadsteads, or waters, do not apply to war-ships devoted exclusively to religious, scientific, or philanthropic purposes.

Art. 15. In the absence of special provisions to the contrary in the legislation of a neutral Power, the maximum number of warships belonging to a belligerent which may be in one of the ports or roadsteads of that Power simultaneously shall be three.

Art. 16. When war-ships belonging to both belligerents are present simultaneously in a neutral port or roadstead, a period of not less than twenty-four hours must elapse between the departure of the ship belonging to one belligerent and the departure of the ship belonging to the other. The order of departure is determined by the order of arrival, unless the ship which arrived first is so circumstanced that an extension of its stay is permissible. A belligerent war-ship may not leave a neutral port or roadstead until twenty-four hours after

the departure of a merchant ship flying the flag of its adversary.

Art. 17. In neutral ports and roadsteads belligerent war-ships may only carry out such repairs as are absolutely necessary to render them seaworthy, and may not add in any manner whatsoever to their fighting force. The local authorities of the neutral Power shall decide what repairs are necessary, and these must be carried out with the least possible delay.

Art. 18. Belligerent war-ships may not make use of neutral ports, roadsteads, or territorial waters for replenishing or increasing their supplies of war material or their armament, or for completing their crews.

Art. 19. Belligerent war-ships may only revictual in neutral ports or roadsteads to bring up their supplies to the peace standard. Similarly these vessels may only ship sufficient fuel to enable them to reach the nearest port in their own country. They may, on the other hand, fill up their bunkers built to carry fuel, when in neutral countries which have adopted this method of determining the amount of fuel to be supplied. If, in accordance with the law of the neutral Power, the ships are not supplied with coal within twenty-four hours of their arrival, the permissible duration of their stay is extended by twenty-four hours.

Art. 20. Belligerent war-ships which have shipped fuel in a port belonging to a neutral Power may not within the succeeding three months replenish their supply in a port of the same Power.

Art. 21. A prize may only be brought into a neutral port on account of unseaworthiness, stress of weather, or want of fuel or provisions. It must leave as soon as the circumstances which justified its entry are at an end. If it does not, the neutral Power must order it to leave at once; should it fail to obey, the neutral Power must employ the means at its disposal to release it with its officers and crew and to intern the prize crew.

Art. 22. A neutral Power must, similarly, release a prize brought into one of its ports under circumstances other than those referred to in Article 21.

Art. 23. A neutral Power may allow prizes to enter its ports and roadsteads, whether under convoy or not, when they are brought there to be sequestrated pending the decision of a Prize Court. It may have the prize taken to another of its ports. If the prize is convoyed by a war-ship, the prize crew may go on board the convoying ship. If the prize is not under convoy, the prize crew are left at liberty.

Art. 24. If, notwithstanding the notification of the neutral Power, a belligerent ship of war does not leave a port where it is not entitled to remain, the neutral Power is entitled to take such measures as it considers necessary to render the ship incapable of taking the sea during the war, and the commanding officer of the ship must facilitate the execution of such measures. When a belligerent ship is detained by a neutral Power, the officers and crew are likewise detained. The officers and crew thus detained may be left in the ship or kept either on another vessel or on land, and may be subjected to the measures of restriction which it may appear necessary to impose upon them. A sufficient number of men for looking after the vessel must, however, be always left on board. The officers may be left at liberty on giving their word not to quit the neutral territory without permission.

Art. 25. A neutral Power is bound to exercise such surveillance as the means at its disposal allow to prevent any violation of the provisions of the above Articles occurring in its ports or roadsteads or in its waters.

Art. 26. The exercise by a neutral Power of the rights laid down in the present Convention can under no circumstances be considered as an unfriendly act by one or other belligerent who has accepted the articles relating thereto.

Art. 27. The Contracting Powers shall communicate to each other in due course all laws, proclamations, and other enactments regulating in their respective countries the status of belligerent war-ships in their ports and waters, by means of a communication addressed to the Government of the Netherlands, and forwarded immediately by that Government to the other Contracting Powers.

Art. 28. The provisions of the present Convention do not apply except between Contracting Powers, and then only if all the belligerents are parties to the Convention.

Art. 29. The present Convention shall be ratified as soon as possible. The ratifications shall be deposited at The Hague. The first deposit of ratifications shall be recorded in a ' procès-verbal ' signed by the representatives of the Powers which take part therein and by the Netherlands Minister for Foreign Affairs. The subsequent deposits of ratifications shall be made by means of a written notification addressed to the Netherlands Government and accompanied by the instrument of ratification. A duly certified copy of the ' procès-verbal ' relative to the first deposit of ratifications, of the ratifications mentioned in the preceding paragraph, as well as of the instruments of ratification, shall be at once sent by the Netherlands Government, through the diplomatic channel, to the Powers invited to the Second Peace Conference, as well as to the other Powers which have adhered to the Convention. In the cases contemplated in the preceding paragraph, the said Government shall

inform them at the same time of the date on which it received the notification.

Art. 30. Non-Signatory Powers may adhere to the present Convention. The Power which desires to adhere notifies in writing its intention to the Netherlands Government, forwarding to it the act of adhesion, which shall be deposited in the archives of the said Government. That Government shall at once transmit to all the other Powers a duly certified copy of the notification as well as of the act of adhesion, mentioning the date on which it received the notification.

Art. 31. The present Convention shall come into force in the case of the Powers which were a party to the first deposit of the ratifications, sixty days after the date of the ' procès-verbal ' of that deposit, and, in the case of the Powers who ratify subsequently or who adhere, sixty days after the notification of their ratification or of their decision has been received by the Netherlands Government.

Art. 32. In the event of one of the Contracting Powers wishing to denounce the present Convention, the denunciation shall be notified in writing to the Netherlands Government, who shall at once communicate a duly certified copy of the notification to all the other Powers, informing them of the date on which it was received. The denunciation shall only have effect in regard to the notifying Power, and one year after the notification has been made to the Netherlands Government.

Art. 33. A register kept by the Netherlands Ministry for Foreign Affairs shall give the date of the deposit of ratifications made by Article 29, paragraphs 3 and 4, as well as the date on which the notifications of adhesion (Article 30, paragraph 2) or of denunciation (Article 32, paragraph I) have been received.

C. Rules in International Law Manuals on Neutrality in Cyberspace

Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations

Rule 150 – Protection of neutral cyber infrastructure
The exercise of belligerent rights by cyber means directed against neutral cyber infrastructure is prohibited.

Rule 151 – Cyber operations in neutral territory
The exercise of belligerent rights by cyber means in neutral territory is prohibited.

Rule 152 – Neutral obligations
A neutral State may not knowingly allow the exercise of belligerent rights by the parties to the conflict from cyber infrastructure located in its territory or under its exclusive control.

Rule 153 – Response by parties to the conflict to violations
If a neutral State fails to terminate the exercise of belligerent rights on its territory, the aggrieved party to the conflict may take such steps, including by cyber operations, as are necessary to counter that conduct.

Rule 154 – Neutrality and Security Council actions
A State may not rely upon the law of neutrality to justify conduct, including cyber operations, that would be incompatible with preventive or enforcement measures decided upon by the Security Council under Chapter VII of the Charter of the United Nations.

Oslo Manual on Selected Topics of the Law of Armed Conflict

Rule 30
A Belligerent State should not conduct cyber operations that constitute attacks causing physical damage to or destruction of objects located in neutral territory, including neutral cyber infrastructure, unless the Neutral State is unable or unwilling to terminate an abuse of such objects or infrastructure by an adversary of the Belligerent State.

Rule 31
Belligerent States must not launch attacks from cyber infrastructure located in neutral territory or under the exclusive control of Neutral States.

Rule 32
If in the context of an armed conflict a Belligerent Party undertakes cyber operations constituting an attack from cyber infrastructure located on Neutral territory, the neutral State must use reasonable means at its disposal to terminate the attack once it becomes aware of it.

Rule 33
The mere fact that cyber operations are routed through neutral cyber infrastructure does not constitute a violation of neutrality.

Rule 34
(a) Without prejudice to Rule 32, the mere use of neutral cyber infrastructure by a Belligerent State is not generally prohibited.
(b) (b) Belligerent States are thus permitted to:
  i. Erect a new cyber communication installation on the territory of a Neutral State that is exclusively used for non-military communications;
  ii. Use an existing cyber communication installation established by them before the outbreak of the armed conflict (including for military communications), provided that it is open for the service of public messages; or
  iii. Use an existing cyber communication installation established by them before the outbreak of the armed conflict and which is not open for the service of public messages, provided it is for non-military communications.

Rule 35
Any measure of restriction or prohibition taken by a Neutral State with regard to the activities referred to in Rule 34 should be impartially applied to all Belligerent States.

D. *Opinio Juris* Quotes

The United States of America

Key Documents or Statements

- 1999 Assessment by the DoD's General Counsel Office[381]
- 2011 US DoD Cyberspace Policy report
- 2012 US Presidential Policy Directive 20
- 2012 Harold H. Koh Remarks on International Law and cyberspace
- 2016 Brian J. Egan Remarks on international law and stability in cyberspace
- 2015 DoD Law of War Manual - section 16.4
- 2020 Paul C. Ney DOD General Counsel Remarks at US Cyber Command Legal Conference
- 2021 Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States

Specific Quotes

- **Scope of application:** The US government will conduct cyber operations "consistent with its obligations under international law, including with regard to matters of sovereignty and neutrality". (2012a, p.4)
- **Impartiality duty and Article 8:** restating Article 8 HC V, it States that "A neutral Power is not called upon to forbid or restrict [communications], so long as such facilities are provided impartially to both belligerents." As a mark of its time, the example provided with this quote relate mostly to communication satellites. (1999, p. 10)
- **Cyber operations through neutral territory or infrastructure:** The use of a "nation's communications networks as a conduit for an electronic attack would not be a violation of its sovereignty in the same way that would be a flight through its airspace by a military aircraft." Nations need not have much concern "for the reaction of nations through whose territory or communications systems a destructive message may be routed.", and "Even if it [the neutral] becomes aware of the transit of such a message and attributes it to the United States, there would be no established principle of international law that it could point to as being violated. […] international law does not require a neutral nation to restrict the use of its public communications networks by belligerents." However, the "(t)ransited State would have somewhat more right to complain if the attacking State obtained unauthorized entry into its computer systems as part of the communications path to the target computer." (1999, p. 22-23)
- **Cyber operations through neutral territory or infrastructure:** "The issue of the legality of transporting cyber 'weapons' across the Internet through the infrastructure owned and/or located in neutral third countries without obtaining the equivalent of 'overflight rights." (2011, p. 8)
- **Cyber operations through neutral territory or infrastructure, impartiality and prevention duty**: However, "merely relaying information through neutral communications infrastructure (provided that the facilities are made available impartially) generally would not constitute a violation of the law of neutrality that belligerent States would have an obligation to refrain from and that a neutral State would have an obligation to prevent"[382] (2015, p. 993)
- **Cyber operations through neutral territory or infrastructure:** "it would not be prohibited for a belligerent State to route information through cyber infrastructure in a neutral State that is open for the service of public messages, and that neutral State would have no obligation to forbid such traffic." "This rule would appear to be applicable even if the information that is being routed through neutral communications infrastructure may be characterized as cyber weapon or otherwise could cause destructive effects in a belligerent State (but no destructive effects within the neutral State or States)." (2015, p. 994)
- **Prevention duty and remedies:** "If a neutral nation permits its information systems to be used by the military forces of one of the belligerents, the other belligerent generally has a right to demand that it stop doing so. If the neutral refuses, or if for some reason it is unable to prevent such use by an belligerent, the other belligerent may have a limited right of self-defense to prevent such use by its enemy."[383] Alternatively, it also has the "right to use force to neutralize a continuing threat located in the territory of a neutral State, but not acting on its behalf, when the neutral State

[381] A First edition was published in May 1999 and a second one in November 1999. These quote are the same in both documents, but the page referencing is that of the first edition.

[382] As the report rightly points out, the original driver behind "communication exception" was because it was viewed impractical for neutral States to censor or screen their publicly available communications infrastructure for belligerent messaging. An analogy that could certainly be made today pertaining to digital communications.

[383] As mentioned in the assessment, this this doctrine has venerable roots in US foreign and defense policy, dating at least to the famous 1837 Caroline incident and the diplomatic crisis that ensued.

is unable or unwilling to execute its responsibility to prevent the use of its territory as a base or sanctuary for attacks on another nation." (1999, p. 10)
- **Remedies against non-State actors using neutral territory:** Coincidently, "(a)ttacks on insurgents or on terrorists and other criminals using a neutral nation's territory as a refuge may also be justified when the neutral State is unable to satisfy its obligations." (1999, p. 22)
- **Considerations for response to hostile cyber operations:** "The issue of third-party sovereignty to determine what to do when the US military is attacked, or US military operations and forces are at risk in some other respect, by actions taking place on or through computers or other infrastructure located in a neutral third country." (2011, p. 8)

The Netherlands

Key Documents or Statements

- Appendix to the letter of 5 July 2019 from the Minister of Foreign Affairs to the President of the House of Representatives on the international legal order in cyberspace.

Specific Quotes

- **Non-participation duty:** "Neutrality requires that States which are not party to an armed conflict refrain from any act from which involvement in the conflict may be inferred or acts that could be deemed in favour of a party to the conflict." (2019, p. 5)
- **Impartiality duty:** "In its relations with parties to the armed conflict the neutral State is required to treat all parties equally in order to maintain its neutrality." It highlighted that denial of access to a neutral State's IT systems must be applied equally to the belligerents. (2019, p. 5)
- **Prevention duty and cyber operations on neutral territory or infrastructure**: "In an armed conflict involving other parties, the Netherlands can protect its neutrality by impeding the use by such parties of infrastructure and systems (e.g. botnets) on Dutch territory. Constant vigilance, as well as sound intelligence and a permanent scanning capability, are required here." (2019, p. 5)

France

Key Documents or Statements

- 2019 Statement from the *Ministère des armées* – section 2.3

Specific Quotes

- **Scope of application**: "Cyberoperations carried out in the context of an international armed conflict, or which trigger such a conflict, are subject to the law of neutrality." It notably quoted the Advisory opinion on the Legality of the Threat or Use of Nuclear Weapons passage on neutrality applying to whatever type of weapons used. (2019, p. 16)
- **Prevention duty and article 8 exception:** "The neutral State must prevent any use by belligerent States of ICT infrastructure situated on its territory or under its exclusive control. However, it is not required to prevent belligerent States from using its ICT networks for communication purposes" (2019, p. 16)
- **Cyber operations against neutral territory or infrastructure**: "Belligerents must refrain from causing harmful effects to digital infrastructure situated on the territory of a neutral State or from launching a cyberattack from such infrastructure." (2019, p. 16)
- **Cyber operations from neutral territory or infrastructure:** "States party to an IAC may neither carry out cyber operations linked to the conflict from installations situated on the territory of a neutral State or under the exclusive control of a neutral State, nor take control of computer systems of the neutral State in order to carry out such operations." (2019, p. 16)
- **Cyber operations through neutral territory or infrastructure:** "Routing a cyberattack via the systems of a neutral State without any effect on that State does not breach the law of neutrality, which prohibits only the physical transit of troops or convoys." (2019, p. 16)

Switzerland

Key Documents or Statements

- 2021 Switzerland's position paper on the application of international law in cyberspace Annex UN GGE 2019/2021

Specific Quotes

- **Scope of application**: "As a matter of principle, Switzerland considers the rights and obligations of neutral countries in international armed conflicts to be applicable to cyberspace as well. It notably quoted the Advisory opinion on the Legality of the Threat or Use of Nuclear Weapons passage on neutrality applying to whatever type of weapons used. (2021, p.4)
- **Limits to the scope of application**: "data are not only transmitted via terrestrial and cable channels but also via satellites located in outer space, which puts them outside the scope of application of the law of neutrality." (2021, p.5)
- **Sovereign right of neutrals**: "Parties to the conflict are obliged in turn to respect the

territorial integrity of the neutral country." (2021, p. 4)
- **Non-participation duty**: "Neutral countries may not support conflicting parties with either troops or their own weapons." (2021, p. 5)
- **Prevention duty**: "a neutral country has a duty to prevent any infringements of its neutrality, such as the use of its territory by one of the conflicting parties." And that "In terms of military cyber operations in connection with an international armed conflict, this means that a neutral country must prevent parties to the conflict from using its military-controlled systems or networks. In general, military networks are shielded and not publicly accessible" (2021, p. 4-5)
- **Cyber operations against neutral territory or infrastructure: "**In principle, belligerent States are not permitted to damage the data networks of neutral countries when undertaking combat operations via their own computer networks." (2021, p.5)
- **Cyber operations from neutral territory or infrastructure**: "Therefore they may not conduct related cyber operations from installations that are either on the territory or under the exclusive control of the neutral country. Parties to the conflict are also prohibited from taking control of a neutral country's computer systems in order to carry out such operations." (2021, p. 4)

Italy

Key Documents or Statements

- 2021 Italian Position Paper on "International Law and Cyberspace" – section 3.d

Specific Quotes

- **Impartiality duty:** "Within an armed conflict, any action taken by a neutral State should be applied equally to all belligerents. For instance, a State may not provide or deny access to its ICT infrastructure to one party but not to the other(s)." (2021, p. 10)
- **Cyber operations from neutral territory or infrastructure**: "According to the law of neutrality, parties to an international armed conflict may not launch wrongful cyber operations from ICT infrastructure located in the territory or under the exclusive control of a neutral State." (2021, p. 21)

Romania

Key Documents or Statements

- 2021 Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States

Specific Quotes

- **Scope of Application:** "We are also of the view that the principle of neutrality apply as well to cyber operations as part of an armed conflict" (2021, p. 78)
- **Cyber operations against neutral territory or infrastructure:** "belligerents must refrain from harming information and communication infrastructure situated on the territory of a neutral State (2021, p. 78)
- **Cyber operations from neutral territory or infrastructure:** "belligerents must refrain […] from launching attacks from such infrastructure." (2021, p. 78)

Denmark

While Denmark has not yet published a general Statement on the application of international law to cyberspace, the Danish Ministry of Defense has stated its views within the updated Military Manual on International Law Relevant to Danish Armed Forces in International Operations.[384] Among other things pertaining to the law of war, the manual explicitly – albeit succinctly – references the law of neutrality and its application to cyberspace within the section on international armed conflicts section.

The document highlights the current lack of State practice concerning the application of neutrality principles in relation to cyberwarfare but presumes that "the principles must generally […] be of relevance in this area."[385] To which it makes a parallel to the classic neutrality rule that provide that neutral infrastructure – private, State-owned, or under its jurisdiction abroad – must not be the object of an attack. It also adds that "infrastructure located in the territory of a neutral State may not be used by belligerent States to engage in acts of war."[386]

Israel

In a keynote speech at the US Naval War College's event on "Disruptive Technologies and International Law on 8 December 2020, Israel's Deputy Attorney General (International Law), Dr. Roy Schöndorf, provided its view on the application of international law to cyber operations. Taking a cautious approach, he underline

[384] Danish Ministry of Defense. (2016). Military Manual on international law relevant to Danish armed forces in international operations. P. 60

[385] Ibid.

[386] Ibid.

the lack of clarity as to the application of the law of neutrality to cyberspace, stating that:

> *"The law of neutrality also illustrates the challenges of applying rules that evolved in the context of traditional warfare to the contemporary environment of cyberspace, as many of its rules were tailored specifically to the land, sea and air domains. For example, in relation to one of the basic overarching rules of neutrality – the inviolability of a neutral State's territory – while in the land domain it is forbidden to transfer troops or convoys of munition; at sea – the passage of warships in territorial waters is possible; and in the air such passage is subject to discretion or limitations of each neutral State. Given these differences, it remains unclear if and how this rule would be applicable in cyberspace."*

E. *Opinio Juris* Sources

Most of the OEWG sources can be found in the following repository.

Country	Title of the Consulted Document	Date	Type
Australia, Brazil, Estonia, Germany, Japan, Kazakhstan, Kenya, Netherlands, Norway, Romania, Russia, Singapore, Switzerland, the United Kingdom, the United States of America	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	2021	Statement of Opinio Juris
Australia	Australia's position on how international law applies to State conduct in cyberspace	2017	Statement of Opinio Juris
Australia	International Law Supplement	2019	Statement of Opinio Juris
Australia	Australia Non Paper Case studies on the application of international law in cyberspace	2020	Statement of Opinio Juris
Australia	Australia's comments on the Initial "Pre-draft" of the report of the UN Open Ended Working Group in the field of information and telecommunications in the context of international security (OEWG)	2020	OEWG contribution
Austria	Pre-Draft Report of the OEWG - ICT Comments by Austria	2019	OEWG contribution
Austria	Comments by Austria on the Zero-Draft for the OEWG's Final Report	2021	OEWG contribution
China	China's Positions on International Rules-making in Cyberspace	2021	Statement of Opinio Juris
Czech republic	Comments submitted by the Czech Republic in reaction to the initial "pre-draft" report of the Open-Ended Working Group on developments in the field of information and telecommunications in the context of international security	2020	OEWG contribution

Czech republic	Statement by Mr. Richard Kadlčák Special Envoy for Cyberspace Director of Cybersecurity Department at the 2nd substantive session of the Open-ended Working Group on developments in the field of information and telecommunications in the context of international security of the First Committee of the General Assembly of the United Nations	2020	OEWG contribution; Statement of Opinio Juris
Czech republic	Statement of the Czech Republic Informal OEWG consultations on the zero draft report	2021	OEWG contribution
Estonia	President of the Republic at the opening of CyCon 2019	2019	Speech/ Keynote by Official
Estonia	Estonia's comments to the OEWG pre-draft report	2020	OEWG contribution
Estonia	Estonia's response to the OEWG zero draft report	2021	OEWG contribution
European Union	EU Statement – United Nations 1st Committee: Thematic Discussion on Other Disarmament Measures and International Security	2018	Statement of Opinio Juris
European Union	Joint comments from the EU and its Member States on the initial 'pre-draft' report of the Open-Ended Working Group on developments in the field of Information and Telecommunication in the context of international security.	2020	OEWG contribution
European Union	Joint comments from the EU and its Member States on the draft report1 of the Open-Ended Working Group on developments in the field of Information and Telecommunication in the context of international security.	2021	OEWG contribution
European Union	Key EU messages, OEWG virtual session on Zero-draft	2021	OEWG contribution
Finland	International law and cyberspace	2020	Statement of Opinio Juris
Finland	Statement by Ambassador Janne Taalas at the second session of the open-ended Working Group (OEWG) on developments in the field of information and telecommunications in the context of international security	2020	OEWG contribution
France	International Law applied to Operations in Cyberspace	2019	Statement of Opinio Juris
Germany	Cyber Security as a Dimension of Security Policy – by Norbert Riedel	2015	Speech/ Keynote by Official

Germany	Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Dr. Alexander S. Neu, Andrej Hunko, Wolfgang Gehrcke, weiterer Abgeordneter und der Fraktion DIE LINKE. BT-Drs. 18/6989	2015	Official Statement
Germany	Initial "Pre-draft" of the report of the OEWG on developments in the field of information and telecommunications in the context of international security	2020	OEWG contribution
Germany	Comments by Germany on the OEWG Zero Draft Report	2021	OEWG contribution
Germany	On the Application of International Law in Cyberspace	2021	Statement of Opinio Juris
ICRC	International Humanitarian Law and Cyber Operations during Armed Conflicts - ICRC position paper	2020	OEWG contribution
Iran	Submission by the Islamic Republic of Iran	2019	OEWG contribution
Iran	General Comments by delegation of the Islamic Republic of Iran on the Revise "pre-draft"	2020	OEWG contribution
Iran	General Staff of Iranian Armed Forces Warns of Tough Reaction to Any Cyber Threat	2020	Speech/ Keynote by Official
Iran	Intervention by delegation of the Islamic Republic of Iran On International Law	2020	OEWG contribution
Iran	Second submission by the Islamic Republic of Iran	2020	OEWG contribution
Israel	Israel's perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations	2020	Speech/ Keynote by Official
Italy	Italian Position Paper on International Law and Cyberspace	2021	Statement of Opinio Juris
Netherlands	International law in cyberspace	2019	Statement of Opinio Juris
Netherlands	Letter of 5 July 2019 from the Minister of Foreign Affairs to the President of the House of Representatives on the international legal order in cyberspace	2019	Official Statement
Netherlands	The Kingdom of the Netherlands' response to the pre-draft report of the OEWG	2020	OEWG contribution
Netherlands	Statement by H.E. Nathalie Jaarsma Kingdom of the Netherlands to the United Nations - Informal virtual meeting OEWG	2021	OEWG contribution
Netherlands	The Netherlands – written proposals to OEWG zero draft	2021	OEWG contribution
New Zealand	Position Paper on New Zealand's Participation in the February 2020 Session of the 2019-2020 Open Ended	2020	OEWG contribution

	Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security		
New Zealand	The Application of International Law to State Activity in Cyberspace	2020	Statement of Opinio Juris
Sweden	Sweden's comments on the Initial "Pre-draft" of the report of the UN Open Ended Working Group	2020	OEWG contribution
Switzerland	Position Paper on Switzerland's participation in the 2019-2020 UN Open-ended Working Group on «Developments in the Field of Information and Tele-communications in the Context of International Security» and the 2019-2021 UN Group of Governmental Experts on «Advancing responsible State behavior in cyberspace in the context of international security»	2020	OEWG contribution
Switzerland	Written feedback by Switzerland to the first pre-draft report of the OEWG	2020	OEWG contribution
Switzerland	General comments on the zero draft of 19 January 2021	2021	OEWG contribution
Switzerland	Switzerland's position paper on the application of international law in cyberspace	2021	Opinio Juris, UN GGE contribution
Switzerland	La Suisse est-elle préparée à une cyberguerre du point de vue de la neutralité ?	2021	Response to a parliamentary interpellation
UN General Assembly	Compendium of Statements in explanation of position on the final report	2021	OEWG contribution
United Kingdom	Cyber and International Law in the 21st Century	2018	Speech/ Keynote by Official
United Kingdom	Non-Paper on Efforts to Implement Norms of Responsible State Behavior in Cyberspace, as Agreed in UN Group of Government Expert Reports of 2010, 2013 and 2015	2019	OEWG contribution
United Kingdom	Contribution by United Kingdom to the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the context of International Security	2020	OEWG contribution
United Kingdom	UK response to Chair's initial 'Pre-draft' of the report of the OEWG on developments in the field of information and telecommunications in the context of international security	2020	OEWG contribution

United Kingdom	UK comments on zero draft report of the OEWG on development in the field of ICTs in the context of international security	2021	OEWG contribution
United States of America	An Assessment Of International Legal Issues In Information Operations	1999	Official document
United States of America	US DoD Cyberspace Policy reports	2011	Official document
United States of America	International Law in Cyberspace - Remarks by Harold Hongju Koh	2012	Speech/ Keynote by Official
United States of America	US Presidential Policy Directive 20	2012	Official document
United States of America	Remarks On International Law And Stability In Cyberspace - Brian Egan	2016	Speech/ Keynote by Official
United States of America	DoD Law of War Manual	2016	Official document
United States of America	DOD General Counsel Remarks at US Cyber Command Legal Conference	2020	Speech/ Keynote by Official
United States of America	United States Comments on the Chair's Pre-draft of the Report of the UN Open Ended Working Group (OEWG)	2020	OEWG contribution

About the Authors

Sean Cordey is a Researcher in the Risk and Resilience Team at the Center for Security Studies (CSS) at ETH Zürich. His research interests include national and European cybersecurity and cyberdefense policy, cyber-enabled influence operations, and international cyber law and norms.

Kevin Kohler is a Researcher in the Risk and Resilience Team at the Center for Security Studies (CSS) at ETH Zurich. His research interests include the use of information and communication technologies in disaster risk management and the long-term trajectory and politics of digital technologies.

CSS
ETH Zürich

The **Center for Security Studies (CSS)** at ETH Zürich is a center of competence for Swiss and international security policy It offers security policy expertise in research, teaching, and consulting. The CSS promotes understanding of security policy challenges as a contribution to a more peaceful world. Its work is independent, practice-relevant, and based on a sound academic footing.