UNIVERSITY OF COPENHAGEN
CENTRE FOR MILITARY STUDIES

Towards Tallinn Manual 3.0

Challenges and Perspectives

Keiko Kono

September 2026

Towards Tallinn Manual 3.0

This report is a part of Centre for Military Studies' policy research services for the Ministry of Defence and the political parties to the Defence Agreement. The purpose of the report is to examine the disagreements and controversies that have arisen regarding the two Tallinn Manuals, 1 & 2, and proposes recommendations for Denmark concerning the positions it should take ahead of Tallinn Manual 3.0.

The Centre for Military Studies is a research centre at the Department of Political Science at the University of Copenhagen. The Centre undertakes research on security and defence issues as well as military strategy. This research constitutes the foundation for the policy research services that the Centre provides for the Ministry of Defence and the political parties to the Defence Agreement.

This report contains an analysis based on academic research methodology. Its conclusions should not be understood as a reflection of the views and opinions of the Danish Government, the Danish Armed Forces or any other authority.

Read more about the Centre and its activities at http://cms.polsci.ku.dk/.

Author:
Dr. Keiko Kono, former Postdoc at the Centre for Military Studies

Editor:
Dr. Kevin Jon Heller, Professor at the Centre for Military Studies

Acknowledgments:
The author is grateful to Brigadier General (Ret.) Jaak Tarien, LtCol (Ret.) Franz Lantenhammer, Professor Marko Milanovic, Mr. Lauri Aasmann, Dr. Bernhards "BB" Blumbergs, Professor Kevin Jon Heller and other colleagues at CMS and the Faculty of Law at the University of Copenhagen for their feedback and comments.

ISBN: 978-87-94550-39-0

Contents

Abstract

The two Tallinn Manuals, which are expert attempts at articulating how international law applies to cyber warfare and operations, have sparked diverse opinions and interpretations across states and scholars. They are important for both state legal advisors and non-legal government staff, as they provide guidance on critical issues pertaining to international law, such as countermeasures, due diligence, collective countermeasures, extraterritorial jurisdiction, and the definition of cyberattacks under international humanitarian law. The report examines the disagreements and controversies that have arisen regarding the two Tallinn Manuals and proposes recommendations for Denmark concerning the positions it should take ahead of Tallinn Manual 3.0.

1 Introduction

1.1 Scope of Research

The *Tallinn Manual on the International Law Applicable to Cyber Warfare*[1] (TM1) and *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*[2] (TM2) are academic endeavors by experts to articulate existing international law relating to state cyber operations based on assessments of state practice. Despite the project being non-governmental and formally politics-neutral,[3] TM1 and TM2 are highly referenced by governments and academia alike, and they are praised as important professional achievements[4] in this field.

Increasing numbers of states have presented position papers on how international law applies in cyberspace, some of which maintain unique interpretations of the subject, and efforts to create a third edition of the Tallinn Manual (TM3) are underway at the time of writing.[5] This report thus aims to present a rough sketch of both manuals to readers in Denmark while also identifying disputed issues that that Denmark must consider ahead of TM3.

Both publications were hosted by the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE)[6] and produced by an international group of experts (IGE) participating in their personal capacity (NATO CCDCOE convened the group). Since its accession to NATO CCDCOE in 2019,[7] Denmark has become one of the supporting states for the Tallinn Manuals and, thus, has a significant interest in how TM3 will progress. At the same time, Denmark is expected to actively contribute to TM3's successful completion.[8]

From a domestic perspective, such background work will also help Denmark to articulate more granular views on how international law applies in cyberspace. As the Danish Ministry of Foreign Affairs released its long-awaited first position paper on the subject in July 2023,[9] its legal interpretations must be fully integrated into all cyber-related government business, including Danish defense and security policies. Although the main audiences of the Tallinn Manuals are "State legal advisors charged with providing international law advice to governmental decision makers, both civilian and military,"[10] the manuals are also of significance to the daily work of other non-legal government personnel, such as when cyberattacks emanating from another state affect election and healthcare policy and other government services. On top of that, any citizen can fall victim to a cyberattack on critical infrastructure, whether to be put at risk of a power outage or manipulated by cyber meddling operations during an election campaign. Those impacted by prospective cyberattacks, therefore, will all benefit from understanding the Tallinn Manuals.

That said, the Tallinn Manuals reflect diverging views on the subject among states and experts. The report thus starts by examining where these disagreements and controversies lie in the two Tallinn Manuals before it proposes recommendations for Denmark. Commentators have already made an abundance of assessments of TM1 and TM2, including the topics of countermeasures, due diligence, and sovereignty.[11] This report thus refrains from investigating these basic concepts thoroughly; instead, it seeks to analyze very

granular aspects of the manuals: how experts agreed or disagreed on selected topics; how their views were of relevance to high-profile cyber incidents that actually occurred in recent years; and the possible impact of state stances on TM3. Building in particular on the preceding academic work on the principle of sovereignty,[12] the report focuses on the following topics: (1) espionage, (2) extra-territorial enforcement jurisdiction, (3) non-intervention, (4) due diligence, (5) collective countermeasures, (6) the plea of necessity, and (7) the notion of "attack" under International Humanitarian Law (IHL).

1.2 Methodology

This article is based on open-sourced research. It references the two Tallinn Manuals together with state position papers on international law on cyber-related issues. The following thirty states have released documents:[13] Australia,[14] Brazil,[15] Canada,[16] China,[17] Costa Rica,[18] Czech Republic,[19] Denmark, Estonia,[20] Finland,[21] France,[22] Germany,[23] Iran,[24] Ireland,[25] Israel,[26] Italy,[27] Japan,[28] Kazakhstan,[29] Kenya,[30] the Netherlands,[31] New Zealand,[32] Norway,[33] Pakistan,[34] Poland,[35] Romania,[36] Russia,[37] Singapore,[38] Sweden,[39] Switzerland,[40] UK,[41] US,[42] and the African Union (AU).[43]

This report is also based on primary sources issued by relevant entities and interviews with those involved in the Tallinn Manuals. The author only received input from a limited number of respondents, presumably due in part to the TM3 project being underway.

1.3 Outline of the Report

The next chapter, Chapter 2, tracks the paths that the Tallinn Manuals have previously followed. It starts with investigation of the host organization of TM1 and TM2 (NATO CCDCOE), as they are known to have driven the process. It then proceeds to the questions of how the Manual stakeholders responded to their deliverables after publication and whether they considered the project's goals achieved. Chapter 3 focuses on points of (dis)agreement among the experts regarding the topics listed above and offers tentative assessments of actual cyber incidents in accordance with relevant TM rules and the different views in state commentaries. Chapter 4 concludes with potential tasks for TM3 and for Denmark to pursue going forward.

2 Overview of the Tallinn Manuals

2.1 History

2.1.1 Cyberattacks on Estonia in 2007

To track the history of the *Tallinn Manuals* properly, one must look back to the 2007 cyberattacks on Estonia as a triggering event. Following a surge of tensions over the Bronze Soldier monument, erected in Tallinn as a symbol of the Soviet victory over Nazi Germany but perceived by many Estonians as a symbol of Communist repression, the Estonian government decided to relocate the statute along with the remains of the Soviet soldiers buried at its original site to the military cemetery in Tallinn in 2007. An Estonian political party with links to the Kremlin, the Russian government and Russian media all condemned the Estonian "fascist government" and "rewriting of history." On April 26, when the preparatory work began, protesters gathered at the site, which escalated into street riots with looting and vandalism in the Estonian capital and in Russia, leading to the death of a young man with Russian citizenship.[44] Protests also erupted in Moscow; the Estonian Embassy in Moscow was besieged by Russian nationalist youth movements, such as the Nashi and Molodaya Rossiya, both of which the Russian government at least passively supported.[45] The safety and immunity of the embassy and its personnel, including the ambassador, were threatened.

The cyberattacks began on April 27 and lasted twenty-two days. The attacks originated from computers in 178 countries but were largely committed by political activists who were coordinated and resourced both financially and intellectually with instructions from Russian hacker sites. Numerous identified IP addresses involved in the attacks were Russians, including Russian state institutions. Nashi activists claimed their involvement, a claim later endorsed by a State Duma Deputy.[46] Technically speaking, the attacks were mild in relation to what Russia *could* otherwise do.[47] But the Denial-of-Service (DoS)[48] and Distributed Denial-of-Service (DDoS) attacks[49] were "unparalleled in size and variety" for Estonia.[50] Estonia had been "one of the world's most connected nations"[51] and had pioneered a lengthy tradition of research and development in this field since Soviet times. Thus, in 2007, Estonia already had an array of IT experts capable of handling cyber incidents. Due to the small size of the country, "everyone knows everyone and gives each other advice,"[52] which made possible an agile, dynamic, and effective defense.[53]

While the Russian government denied involvement in the attacks, hostile rhetoric from high-ranking Russian politicians and the government's refusal to stop the attacks were believed to embolden the attackers.[54] Moreover, then-Estonian President T. Hendrik Ilves claimed that every internet service provider in Russia was required by law to connect its cables with the Federal Security Service (FSB), which controls the internet nationwide. In Estonia's view, the Russian government was thus indirectly responsible for the attacks.[55]

The Estonian government did not regard the incident as "an armed attack" under Article 51 of the UN Charter, nor it did request invocation of Article 5 of the North Atlantic Treaty.[56] However, the 2007 attacks made the Estonian government more serious about its readiness, which led to the implementation of the National Cyber Security Strategy and creation of the "Cyber Defence League."

In the wake of the incident, NATO provided emergency assistance to Estonia[57] and approved its first Policy on Cyber Defence in January 2008. On April 3 of the same year, NATO heads of state and government issued the Bucharest Summit Declaration, which "paved the way for the establishment of Estonian COE [NATO CCDCOE],"[58] endorsing the Policy on Cyber Defence in the following paragraph on cyber defence:

> 47. NATO remains committed to strengthening key Alliance information systems against cyber attacks. We have recently adopted a Policy on Cyber Defence, and are developing the structures and authorities to carry it out. Our Policy on Cyber Defence emphasises the need for NATO and nations to protect key information systems in accordance with their respective responsibilities; share best practices; and provide a capability to assist Allied nations, upon request, to counter a cyber attack. We look forward to continuing the development of NATO's cyber defence capabilities and strengthening the linkages between NATO and national authorities.[59]

Armed conflict between Russia and Georgia erupted that summer, which further demonstrated how cyberattacks can potentially become a major component in conventional warfare.[60] Although the cyberattacks were DDoS-type attacks and the defacement of Georgian government websites, the fact that cyber means were used for the first time in sync with conventional military operations in an actually fought war[61] likely convinced NATO CCDCOE member states about the pressing need to explore legal issues arising from state cyber operations.

2.1.2 Birth of NATO CCDCOE

The idea of creating a cyber defense hub in Estonia as a new NATO Centre of Excellence (CoE) was proposed by Estonia no later than 2004, when it achieved accession to NATO.[62] In May 2008, seven NATO allies (Estonia, Germany, Italy, Latvia, Lithuania, Slovakia and Spain) and the Allied Command Transformation (ACT) signed the documents to establish a NATO CCDCOE in Estonia as the 9th accredited CoE.[63] The CoE became fully operational in late October that year.[64] From the beginning of its operation, Estonia as the framework nation keenly pursued the Tallinn Manual project for NATO CCDCOE. The proposal to that effect was approved along with other projects at the NATO CCDCOE Steering Committee (SC) meeting[65] around 2008, and NATO CCDCOE asked Professor Michael Schmitt, who had published an article on the topic in 1999,[66] to take charge.[67]

2.1.3 Launch of the Tallinn Manual

(1) TM1 (2009–2013)

The project kicked off in 2009. To produce TM1, an International Group of Experts (IGE)—subject-matter experts with different backgrounds[68]—was convened. Some of the legal experts were authors of renowned international law manuals in the areas of non-international armed conflict[69] and air and missile warfare.[70] In addition to these scholars of international law, the IGE also included technical experts. The TM1 editorial committee had a member specialized in computer science and electrical engineering, his role for TM1 thus being lead technical advisor.[71] NATO CCDCOE also provided technical counsel, as it deployed in-house technical researchers to the IGE. NATO CCDCOE also assumed the roles of managing and coordinating the project.

TM1 was published in 2013. As the title indicates, TM1 focuses on both *jus ad bellum* (law governing use of force by states) and *jus in bello* (IHL).[72] The book consists of two parts. Part I, on International cyber security law, starts with Chapter 1 on states and cyberspace, which deals with basic legal concepts such as sovereignty, jurisdiction and state responsibility. Chapter 2 is about prohibition of the use of force, self-defense against armed attack, and actions of international governmental organizations. Part II, on the law of cyber armed conflict, comprises five chapters in total: Chapter 3 on IHL generally; Chapter 4 on the conduct of hostilities; Chapter 5 on certain persons, objects, and activities; Chapter 6 on occupation; and Chapter 7 on neutrality.

Throughout the entire period, the TM project remained on the agenda of the UNSC meeting and was followed by the NATO CCDCOE member states. Meanwhile, Hungary, the Netherlands, Poland and the U.S. completed the process of joining NATO CCDCOE, bringing the total number of sponsoring nations to eleven when TM1 was published in 2013.[73] However, there was no interactive dialogue regarding the content between the IGE and NATO CCDCOE member states during the drafting process, as "States maintained a distance from the work of the International Group of Experts."[74]

(2) TM2 (2013–2017)

NATO CCDCOE and the Director of *the Tallinn Manual* were both determined to continue the follow-up project even before having completed editing the first edition. To create a smoother process, they carefully planned how to proceed with the second edition. NATO CCDCOE, for instance, surveyed publicly available book reviews, academic articles, and any other analyses of the first edition. Some of these reviews pointed out that the TM1 focus was very narrow, that so-called "cyber warfare" has not occurred, and many more important topics required further study.[75]

To fulfill these expectations by addressing cyber operations below the level of the use of force, new chapters were produced for TM2. TM2 consists of four Parts. Part I includes five chapters: sovereignty, due diligence, jurisdiction, law of international responsibility, and cyber operations not per se regulated by international law (peacetime espionage). Part II, on specialized regimes of international law and cyberspace, has six new chapters: international human rights law, diplomatic and consular law, law of the sea, air law, space law, and international telecommunication law. Part III, on international peace and security, and cyber activities, has both new chapters and updated TM1 chapters: peaceful settlement, prohibition of intervention, the use of force,

and collective security. The structure and rules of Part IV, on the law of cyber armed conflict, are almost the same as TM1.

For the purpose of drafting TM2, a new IGE was convened. A few TM1 experts remained on the IGE, but new experts were also invited from additional western and non-western states, including China, India, Israel, Japan, South Korea and Thailand. The new IGE drastically revised the first chapter of TM1, while TM1 chapters on both *jus ad bellum* and *jus in bello* were reviewed and updated as necessary by TM1 experts and combined in the second edition.

Another innovation for TM2 was a consultation (engagement) process that asked states to "unofficially comment on the working drafts of the Manual in a Chatham House environment."[76] The process was initially designed by NATO CCDCOE and the TM Director to include insights from NATO CCDCOE member states in a draft text of TM2. The scope of eligible participants was later expanded to invite any state that wished to attend. Hosted by the Ministry of Foreign Affairs of the Netherlands, it was ultimately named the "Hague Process." Over fifty nations, including China and Russia,[77] and international organizations attended the process, which involved three two-day sessions.[78]

(3) Characteristics and Structure of the Tallinn Manuals

Both TMs are intended as "a reflection of the law as it existed at the point of the Manual's adoption by the two International Groups of Experts" and "policy and politics-neutral"; hence, not an official view of NATO CCDCOE, its sponsoring states or NATO.[79]

When it comes to identifying the substance of international law, it is nothing new for a group of subject-matter experts acting in their personal capacity to engage in a project to codify the content of international law. Another example is the *San Remo Manual on International Law Applicable to Armed Conflicts at Sea*. In reference to "The Role of Various International Bodies," the editors note that "the regulations, draft rules, resolutions, and reports adopted by them, although not possessing legally binding force, have played, and continue to play, an important role in clarifying the content of pre-existing customary or treaty law, and in influencing the development of the law."[80] The Institute of International Law (IIL), the International Law Association, the International Institute of Humanitarian Law (IIHL), and the International Committee of the Red Cross are named as such organizations. The aim of the San Remo Manual is cited as follows: "[a] contemporary manual was considered necessary because of the developments in the law since 1913 [when the Oxford Manual was adopted by the IIL] which for the most part have not been incorporated into recent treaty law."[81]

In respect to the structure of the Tallinn Manuals, each edition consists of two elements: black-letter rules and accompanying commentary. The black-letter rules, which are printed in bold in the manuals, are adopted unanimously by the TM IGE and "reflect customary international law (unless they expressly reference a treaty) as applied in the cyber context"; or, in other words, "the lex lata[82] instead of the lex ferenda,[83] best practice or preferred policy."[84] They are thus designed to be binding on all states by virtue of customary international law.[85] In turn, the commentary indicates each rule's legal basis, its normative content and practical implications in the cyber context; and above all, the different positions among TM experts, observers, states, and external experts concerning the scope or interpretation of the rule.[86]

In respect to the commentary, TM Director Schmitt explains the benefits of recording different interpretations therein as follows: "understanding the points about which application and interpretation are subject to disparate views allows States to focus their efforts where clarification of the law is needed and in their national interest."[87] As chapter 3 reveals, Schmitt estimates that "certain States are embracing legal ambiguity as a force multiplier in their cyber operations," and especially Russian cyber-meddling operations are exploiting "a grey zone of normative uncertainty" in relation to rules of sovereignty and non-intervention.[88] In his view, the clarification of the law will contribute to deterring such exploitation, "because internationally wrongful acts may be responded to by means of countermeasures" and also prevent escalation.[89]

2.2 Contextualizing the Tallinn Manuals

2.2.1 Impact of the Tallinn Manuals

Both versions of the Tallinn Manual were received with satisfaction by NATO CCDCOE, its member states, and elsewhere. The manuals and their by-products (described below) contribute to raising the level of readiness and familiarity needed by the government experts of member states in charge of legal matters related to cyber operations.

NATO CCDCOE, as a NATO Centre of Excellence tasked with training NATO ally officers, launched a week-long training course on international law in cyberspace at NATO School Oberammergau, Germany, in 2012, then moved the venue to Tallinn the following year. The course had more than 500 participants. Delivered mainly by the TM director and other TM experts, the course is designed to help a range of cyber experts working for the government of each NATO CCDCOE member state (thirty-nine states, as of October 2023), and other candidate states learn various issues concerning the application of international law in cyberspace.

The Tallinn Manuals are also integrated with other NATO CCDCOE projects; for example, cyber defense exercises such as Locked Shields include the legal track aimed at training legal officers of participating countries ("Blue team") to resolve legal issues and provide proper legal counsel to their commander during live-fire cyber defense exercises. Similarly, "International Cyber Law in Practice: Interactive Toolkit" is a spin-off project launched at NATO CCDCOE in 2017. Its aim is to "examine the applicability of international law to the scenarios" that were based on real-world cyber incidents[90] so that anyone can learn various topics of international law arising from particular cyber incidents.

Viewed from a wider perspective, there is one more noticeable impact of the Tallinn Manuals in relation to sources of international law: International law is predominantly state-created. Treaties (conventions) and custom are the only formal (and most important) sources of international law, as listed in Article 38 (1) of ICJ Statute below.[91]

a) *international conventions, whether general or particular, establishing rules expressly recognized by the contesting states;*

b) *international custom, as evidence of a general practice accepted as law;*

c) *the general principles of law recognized by civilized nations;*

d) judicial decisions and the teachings of the most highly qualified publicists of the various nations, as subsidiary means for the determination of rules of law.

Treaties are sources of obligation under law, since they are binding only on states that have chosen to become contracting parties to them. Customary law comprises two elements: first, widespread and consistent state practice, and second, "a belief in legal obligations," called *opinio juris*, and binds all states save for the persistent objector.[92] In addition to these two primary sources of international law, the ICJ and other international tribunals employ general principles of law recognized by civilized nations.[93]

Lastly, as "subsidiary means for the determination of rules of law," and as a persuasive guide to the content of international law, Article 38(1)(d) lists two categories:[94] judicial decisions[95] and the teachings of the most highly qualified publicists of the various nations. The Tallinn Manuals are intended to have the latter status.[96] TM1 and TM2 are often referenced in position papers and military manuals released by states. While states do not uniformly agree with all of the rules in the manuals, they are undoubtedly of significant assistance to states when they decide their own positions.

2.2.2 Launch of TM3

As the preceding sections have shown, the Tallinn Manuals are the result of evolving processes involving various stakeholders. And they continue to evolve to this day. After a set of consultations among stakeholders on the topic, format and other options, the TM3 project was launched in 2021 as a five-year venture with a view to revising and updating TM2. Like the second edition, the same preparatory work—including surveying reviews, relevant articles and most importantly any relevant state practice—has been repeated, and a state engagement process is scheduled to be held again in a few years. Like the previous two editions, NATO CCDCOE funds and manages TM3, providing wide-ranging support to assist the director and co-editors. And for the first time, the process is open to readers, who can submit suggestions directly to TM3 drafters.[97]

TM2 Director Schmitt and TM3 Co-General Editor Marko Milanovic have said that industrial espionage, international criminal law, international environmental law and international investment law are potential new chapters in TM3. Schmitt has also mentioned international human rights law as a core area to be updated in TM3, as he believes TM2 treated this topic unsatisfactorily.[98]

2.2.3 Lex Lata Status of the Tallinn Manuals

As stated in 2.1.3(3), the Tallinn Manuals are designed to be "an objective restatement of the *lex lata*"[99] in the cyber context. In other words, "[t]he Rules that appear in the Manual are those which, by consensus, the International Group of Experts found to apply in cyberspace as a matter of customary law."[100] As an example, what follows is a comparison between Rule 66 of TM1, Rule 89 of TM2, and relevant IHL articles concerning the status of military spies during an international armed conflict.

(1) TM1

Looking back on the history of IHL, the regulation of wartime espionage dates back to Articles 29 and 31 of Convention (IV) respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land of 1907 (Hague Regulations).[101]

Hague Regulations of 1907

Article 29

A person can only be considered a spy when, acting clandestinely or on false pretences, he obtains or endeavours to obtain information in the zone of operations of a belligerent, with the intention of communicating it to the hostile party.[102]

Article 31

A spy, after rejoining the army to which he belongs, is subsequently captured by the enemy, is treated as a prisoner of war, and incurs no responsibility for his previous acts of espionage.

In terms of geographical elements, the phrase "the zone of operations of a belligerent" in Article 29 of the Hague Regulations was expanded in Article 46(2) of API to cover all "territory controlled by an adverse Party: national or occupied territory, area of operations (on land, at sea, or in the air), including the territorial sea."[103]

Article 46 of Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (API) of 1977 (API)[104]: Spies

1. Notwithstanding any other provision of the Conventions or of this Protocol, any member of the armed forces of a Party to the conflict who falls into the power of an adverse Party while engaging in espionage shall not have the right to the status of prisoner of war and may be treated as a spy.
2. A member of the armed forces of a Party of the conflict who, on behalf of that Party and in territory controlled by an adverse Party, gathers or attempts to gather information shall not be considered as engaging in espionage if, while so acting, he is in the uniform of his armed forces.[105]

To date, a total of 176 states support the expansion to that effect as contracting parties to API.

TM1 Rule 66: Cyber Espionage

(a) Cyber espionage and other forms of information gathering directed at an adversary during an armed conflict do not violate the law of armed conflict.
(b) A member of the armed forces who has engaged in cyber espionage in enemy-controlled territory loses the right to be a prisoner of war and may be treated as a spy if captured before re-joining the armed forces to which he or she belongs.

While Rule 66 of TM1 does not transpose Article 46 of API word-for-word, it can be observed that essential elements in both paragraphs of API Article 46 are integrated into TM1 Rule 66(b). Its commentary notes that the cyber ac-

tivity "must occur in territory controlled by a party to the conflict"[106] to constitute espionage. In other words, other cyber operations, such as "CNE and cyber reconnaissance are not cyber espionage when conducted from outside enemy-controlled territory."[107] TM1 contends that this extension is supported as a matter of customary law.[108] As proof of its customary law status, TM1 cites state practice of a non-contracting party to API; that is, *The Commander's Handbook on the Law of Naval Operations* (2007).[109]

Presumably, the ICRC supports TM1 Rule 66. After thorough survey of all relevant documents, including treaties, state-issued non-binding documents, and state military manuals, the 2005 ICRC study on customary IHL concludes that ICRC Rule 107 on spies "applies only to a spy captured in the act whilst in enemy-controlled territory," [110] repeating the phrase of Article 46 of API. TM1 experts must have been aware of the ICRC study while drafting TM1, as TM1 invited the ICRC legal officers to IGE as observers.

(2) TM2

Rule 89 of TM2 below is an outcome of the updating by TM1 experts. Only paragraph (b) of TM1 Rule 66 is succeeded by TM2 Rule 89, despite the same topic. Paragraph (a) of TM1 Rule 66, which is also a well-settled point under IHL, is downgraded into the commentary's paragraph 5 of Rule 89 in TM2.

TM2 Rule 89: Spies

> A member of the armed forces who has engaged in cyber espionage in enemy-controlled territory loses the right to be a prisoner of war and may be treated as a spy if captured before rejoining the armed forces to which he or she belongs.[111]

TM1 experts also updated the evidence of customary international law when editing TM2. As a result, reference to the U.S. military manual is replaced with the most recent version at that time (i.e., the *U.S. DoD's Law of Manual of 2015*, updated in December 2016).[112]

While some authors criticize the same rule in the Tallinn Manual as not taking technical difficulties into consideration,[113] what TM1 experts did regarding the topic of spying under IHL is not law-making, but simply an extension to the cyber domain of what has been regarded as customary international law in the physical context.

3 Selected Topics in the Tallinn Manuals 1 & 2

This chapter examines several topics that were intensely debated by the *IGE*, their observers, external scholars and states: peacetime espionage, extra-territorial enforcement jurisdiction, non-intervention, due diligence, collective countermeasures, the plea of necessity and the notion of attack under IHL.

These seven topics are related to this article's objective: to identify future tasks for Danish legal policy. TM2 was finalized by around June 2016, so the question arises as to whether and to what extent it will be able to present valid yardsticks for legally tackling cyber incidents that occurred since then, such as Russian cyber meddling in the American 2016 presidential election; cyberattacks on the healthcare sector amid the COVID-19 pandemic; disruptive ransomware attacks in a war in Ukraine and its indiscriminate effects beyond the war zone; and cross-border counter-ransomware operations by victim states. For some rules, the interpretation or black-letter statements may change, depending on how states view actual cases. For these reasons, the following depiction in this chapter shows not only the majority views in the TM2 commentaries, but also the minority ones; and even views suggested by various TM directors in their scholarship.

3.1 Peacetime Espionage

The starting point for the discussion is the principle of sovereignty, which is defined as supreme authority within a territory and is a pivotal principle in modern international law.[114] Rule 4 of TM2 provides as follows.

TM2 Rule 4: Violation of Sovereignty

> A state must not conduct cyber operations that violate the sovereignty of another state.[115]

TM2 formulated two bases for assessing whether sovereignty has been violated. The first is the degree of infringement upon territorial integrity (e.g., physical damage, loss of functionality). Regarding loss of functionality, however, TM2 experts could not reach agreement on the precise threshold due to the lack of expressions of *opinio juris* in this regard.[116] The second basis is an interference with or usurpation of inherently governmental functions. TM2 experts agreed that because a state has the exclusive right to perform such functions, deleting or altering data leading to an interference with a particular function violates sovereignty. Listed examples are social services, elections, the collection of taxes, diplomacy and the performance of key national defense activities.[117]

In addition to the unsettled nature of the standards by which to determine the violation of sovereignty, solving the cyber espionage topic is even more complex, as discussed below. As TM2 notes, "[b]y styling a cyber operation as 'cyber espionage operation,' a State cannot therefore claim that it is

by definition lawful under international law."[118] If that is the case, the legality of peacetime cyber operations is simply assessed in accordance with the bases described above. However, at least a few TM2 experts take the different view that state practice of espionage on the territory of a target state without any legal justification is so extensive as to create an exception to the principle of sovereignty. In their view, espionage operations, including by cyber means, whether done remotely or on-site, are lawful unless the operations cause damage, deletion, or alteration of data.[119]

3.1.1 TM1 & 2

(1) TM1

TM1 refers to peacetime cyber espionage in the Rule 6 commentary on the legal responsibility of States, noting that as "international law does not address espionage *per se*… a State's responsibility is not be [sic] engaged as a matter of international law unless particular aspects of the espionage violate specific international legal prohibitions (as in the case of cyber espionage involving diplomatic communications, Rule 84)."[120]

(2) TM2

TM2 created a dedicated rule on the topic and Rule 32's black-letter rule follows the same idea as TM1.

TM2 Rule 32: Peacetime Cyber Espionage[121]

> Although peacetime cyber espionage by states does not violate international law per se, the method by which it is carried out might do so.

The black-letter rule derives from a conviction that "insufficient State practice and *opinion juris* on the matter exits to… conclude [that] a new customary international law norm prohibiting it has crystallized."[122] TM2 experts also agreed that an act of cyber espionage operation breaches the sovereignty of the target state when the method/manner of the operation causes damage or a loss of functionality to a target cyber infrastructure.[123] This conclusion is unchanged when cyber espionage operations bring unintended consequences, such as when the installation of a backdoor resulted in unexpected damage to the target system.[124] In addition, although not described in the Rule 32 commentary, cyber espionage will also be judged a sovereignty violation when it "interferes with data or services that are necessary for the exercise of inherently governmental functions." By "interferes," TM2 means actions beyond mere access to a system or exfiltration of inherently governmental data; further acts are required, such as "changing or deleting such that it interferes with the delivery of social services, the conduct of elections, the collection of taxes, the effective conduct of diplomacy, and the performance of key national defence activities."[125]

On the other hand, TM2 experts were divided on the following three issues. First, regarding "remote cyber espionage reaching a particular threshold of severity [of the consequences suffered]," such as an exfiltration of gigabytes of classified data from state's military cyber system over an extended period. The majority denied illegality, arguing that only the method matters,

while the minority was in the affirmative ("the exfiltration of nuclear launch codes" is a violation of sovereignty).[126]

The second issue is "close access cyber espionage operations, such as an insertion of a USB flash drive into a computer on one State's territory by" an agent of another state. This is an extension and repetition of the discussion made in relation to the principle of sovereignty. The majority of TM2 experts considered it unlawful because of non-consensual presence on the territory of the target state, while a few experts drew the opposite conclusion, claiming that it is permissible as an exception to the sovereignty as well as intervention.[127]

The third point of disagreement is about how to view espionage operations in "a single plan," such as when a state acquires the credentials for the system of another state's nuclear power plant through cyber espionage and then threatens the target state with cyber operations against the system that would cause significant damage or death. According to the majority view, the cyber espionage operations can violate international law, as they are "an integral and indispensable component of an operation." However, the minority view suggested that the espionage aspect should be assessed separately and should thus not be deemed unlawful.[128]

By contrast, TM2 experts were unanimous concerning a case in which a preceding espionage operation and ensuing kinetic attack on another state are distinct, even if the former facilitates the latter. When a state uses the previously gathered intelligence to execute a plan to attack another state with use of force, the cyber espionage is not itself unlawful, according to all TM2 experts.[129] This point is reminiscent of the SolarWinds incident,[130] which has been assessed as an espionage operation "although the backdoor may provide a future opportunity to exploit the vulnerability."[131] The same holds true for another Russian military hacking group, Sandworm. They are reportedly behind a series of cyberattacks, including two against Ukrainian power grids, the Opening Ceremonies at the 2018 Winter Olympics, NotPetya,[132] implanting malware in the U.S. electric grid,[133] and continuously analyzing the internet for vulnerabilities and compiling them for possible future attacks. TM2 experts pointed to the risk facing a target state that cyber espionage is not easily distinguishable from offensive cyber operations, which can lead to misunderstandings.[134]

The fourth point of division is about the use of a honeypot that "will cause significant disruption or damage in the target system." A honeypot is a system (e.g., a web server) or system resource (e.g., a file on a server) designed to be attractive to potential crackers and intruders, like honey attracts bears.[135] TM2 experts were divided on whether the operation is attributable to the state that set it. The minority affirmed this attributability to the user state and a consequent violation of the sovereignty of the target state, although the majority argued the opposite position.[136]

3.1.2 Case Studies

TM2 does not cite particular cyber espionage incidents in the commentary to Rule 32. As a substitute, an analysis of Russian hacks of Democratic National Committee (DNC) servers by TM's Director Schmitt is worth recalling, as his argument was developed based on the TM2. The DNC hack was renowned for being part of a wider election-meddling campaign. An election is a typical example of an inherently governmental function for both the rule of sovereignty and the *domaine réservé* principle of non-intervention.

According to the U.S. Intelligence Community's declassified version of a report released by the Office of the Director of National Intelligence (ODNI) in January 2017[137] and an indictment by the U.S. Department of Justice against Russian entities, upon which Schmitt based his main arguments, Russian Main Intelligence Directorate (GRU)'s cyber operations targeting the U.S. presidential election began by March 2016 and resulted in personal e-mail accounts of Democratic Party officials and other figures being compromised. GRU then exfiltrated large volumes of data from the Democratic Congressional Campaign Committee (DCCC), the DNC, and some of presidential candidate Hillary Clinton's campaign staffers, meaning that most of the hacked data was not governmental or necessary for inherently governmental functions.

Schmitt highlighted the following sequence of facts as aspects falling within the legal grey zone: Russian operations were not just espionage, but also involved the "weaponization" of hacked data through the release to Guccifer 2.0 and DCLeaks.com, both of which had Russian origins, and WikiLeaks, with which the Kremlin's media outlet RT has actively collaborated, "at critical points in the election." Moreover, these websites were promoted by dubious accounts on social media, such as bots and fake American accounts, all of which were Russian creations.[138] Thus, Schmitt suggested that "the trolls sought to bolster that message by feigning the source thereof" and "[a]rguably, this manipulation of voters' ability to assess the messages in coming to their own decision tipped the scales and therefore constituted unlawful interference [with an inherently governmental function],"[139] in the sense that "activities … disturb the territorial State's ability to perform the functions as it wishes."[140]

The DNC hack seems to be "an integral and indispensable component" of a single campaign of Russian meddling operation against the 2016 U.S. election. The majority of TM2 experts concluded that cyber espionage is unlawful as part of a single plan when employed to facilitate a subsequent illegal act,[141] but all TM2 experts agreed that it is not unlawful if it is completely separate from the subsequent illegal act.[142] It makes sense that the Russian hacking of local election boards was not thought of as interference, "for there was no subsequent activity that exploited the access to affect the elections."[143]

Assume here that the minority view is more tenable. They argued that the legality of a cyber espionage operation should be assessed separately, even if it is part of a single plan and the hacking and exfiltration is not unlawful per se. The remaining part of the Russian campaign might still breach the rule of sovereignty to the extent that it interfered with inherently governmental functions. In the case of the U.S. election meddling in 2016, hacked documents did not include ballots or other data necessary for inherently governmental functions, and there was no allegation in the Department of Justice indictment that the operations "altered the vote count or changed the outcome."[144] Hence, it is possible to conclude that there was no interference with the election[145] and thus no violation of sovereignty. The crux of the matter is whether hacked data that is not governmental or necessary for the exercise of inherently governmental functions can nevertheless fatally disturb the proper operation by the target state of its inherently governmental functions. If conceivable, more cases of initial hacking will be assessed as unlawful.

On the other hand, it is a fact-driven assessment about whether cyber espionage operations are independent or an integral part of a single plan. A series of campaigns might be launched over time, like the DNC hack, in which

the hacking took place about nine months after the GRU initially gained access. Especially when a state is notorious for causing damage or dysfunction to critical infrastructure with cyber means, a target state will become more cautious as to how to characterize a malicious cyber espionage operation detected in their systems.

Needless to say, the controversies shown above may not always be relevant to all espionage cases. The question still remains to be resolved whether and under what conditions cyber espionage operation is lawful *per se* under international law. However, TM3 will likely follow the same rule as TM1 and TM2, given their approach that cyber espionage is not prohibited unless a new customary international law prohibition is formed. It is not easy to prove either that extensive and virtually uniform state practice has developed, including that of states whose interests are specially affected, or that general recognition of a legal obligation is involved.[146]

3.1.3 State Positions

(1) For

Canada,[147] Costa Rica,[148] France,[149] New Zealand,[150] Norway[151] and the U.S.[152] are explicitly adopting the view of TM2 rule 32.

(2) Against

China is an unambiguous example of declaring cyber espionage as unlawful. It asserts that "[n]o State shall engage in ICT-enabled espionage or damages against other States, including mass surveillance and theft of important data and personal information."[153] Iran[154] and Switzerland[155] leave room for interpretation, since they do not refer to "espionage." The first two states, in particular, state that "non-consensual or unlawful intrusion" to cyber infrastructure is a violation of sovereignty, while Switzerland notes that "state sovereignty protects information and communication technologies (ICT) infrastructure on a state's territory against unauthorised intrusion or material damage." The African Union also seems to reject the legality of espionage for the same reason.[156]

(3) No Position

The following States have made no reference to the topic of espionage in their published statements: Australia, Brazil, Czech Republic, Denmark, Estonia, Finland, Germany, Ireland, Israel, Italy, Japan, Kazakhstan, Kenya, the Netherlands, Pakistan, Poland, Romania, Russia, Singapore, Sweden, and the UK. While silent in its position paper, Brazil is referred to in TM2 as a state that condemned mass surveillance in the context of a violation of sovereignty.[157] It goes without saying that silence means neither acceptance nor rejection. Insofar as there is room for interpretation that a certain transborder cyber operation does not violate the sovereignty of another state, states will freely engage in cyber operations, including espionage toward another state without any legal justification.

3.1.4 Summary

As for the (un)lawfulness of cyber espionage, TM2 followed the widely accepted view that there is no prohibition of espionage *per se*, but it concluded that espionage may be unlawful when conducted in the manner/method that violates other rules such as the threat or use of force, non-intervention, or

sovereignty. Moreover, according to the dominant view in TM2, espionage is unlawful when part of a single plan and ensuing acts breach the above rules. Previous cases of alleged manipulation of electorates with hacked data is raising a new issue concerning whether only an interference with data necessary for the exercise of inherently governmental functions can violate sovereignty. If other data can be utilized in a manner that harms the proper operation of inherently governmental functions, as in the U.S. cyber election meddling, where hacked data is abused through influence operations on the internet, more cases of preceding cyber espionage will be likely assessed as unlawful.

3.2 Principle of Non-Intervention

Non-intervention is a firmly established principle of international law, according to which no state should intervene in the affairs of another, including by means of ICT. In the *Nicaragua* case, the ICJ determined that the principle is "part and parcel of customary international law."[158] The non-intervention principle is listed as a binding principle of international law in the UN cyber GGE Report of 2021.[159]

3.2.1 TM1 & 2

(1) TM1

There is no black-letter rule on the non-intervention principle in TM1, but its commentary on Rule 10, concerning the prohibition of threat or use of force, devoted five paragraphs to the subject. Cases of prohibited intervention cited there include "supplying funds to insurgents,"[160] which originated from the *Nicaragua* judgement and was thus uncontroversial. Other examples are "all uses of forces," like Stuxnet, "because all uses of force are coercive *per se*."[161] With regard to acts below the use of force, prohibited interventions include "[a]cts meant to achieve regime change" and "the manipulation by cyber means of elections or of public opinion on the eve of elections, as when online news services are altered in favour of a particular party, false news is spread, or the online services of one party are shut off."[162] It is remarkable that TM1 already had cyber-enabled manipulation of public opinion in mind.

(2) TM2

Table 7:
Rule 66: Intervention by States[163]

A State may not intervene, including by cyber means, in the internal or external affairs of another State.

(a) Elements of Intervention: *Domaine Réservé*

As is well known, there are two requirements for a prohibited intervention: domaine réservé and coercion. As for the first element, "the act in question must relate to matters that involve the internal or external affairs of the target State,"[164] including the "choice of a political, economic, social, and cultural system, and the formulation of foreign policy."[165]

Questions are sometimes raised as to how distinct the two following concepts are: "an inherently governmental function," which is a condition for a violation of sovereignty, and domaine réservé. Schmitt explains that despite overlapping, the former is "an activity for the government alone," whereas

the latter is "one that has not been committed to international law by either treaty or customary law."[166] Elections are an example belonging in both categories. Schmitt goes on to discuss an example of cyberattacks on the healthcare sector amid the pandemic in a co-authored article with newly joined TM3 Co-General Editor Marko Milanović:

> Although health care is sometimes provided exclusively or primarily by the state, as in the case of the National Health Service in the United Kingdom, this is not universally the case. Because providing medical care is not an inherently governmental function, cyber operations by states that interfere with the provision of health care in another, even if that victim state does provide health care to its own population, do not, on that basis alone, amount to a sovereignty violation.
>
> However, crisis management during an epidemic or a pandemic is a governmental responsibility in every state and accordingly an inherently governmental function. Any cyber operation attributable to a state that disrupts another state's crisis management planning and execution during a pandemic, at any level of government, therefore qualifies as a sovereignty violation.[167]

These arguments suggest that the healthcare sector in a time other than the crisis can be regarded as domaine réservé but not as "an inherently governmental function." The same logic may also apply to critical infrastructure in other sectors. Given the lack of specification in TM2, it is uncertain which areas should fall within this category. For instance, language policy, more specifically regarding a state's choice of official language(s), seems like both categories, as shown in the commentary to TM2 Rule 66 in which DoS operations from one state to another to enforce the change of the official language policy in the latter state were suggested to be a prohibited intervention.[168] But management/implementation of an education curriculum concerning official language(s) may be no more of an inherently governmental function than peacetime healthcare is.

(b) Elements of Intervention: Coercion

With regard to coercion, TM2 experts elaborated a number of points. For instance, they asserted that non-physical acts can qualify as coercion, such as blocking access to a particular online service,[169] DDoS operations,[170] or a threat of a cyber operation.[171]

TM2 experts were nevertheless divided over three issues. First, according to the majority view, "the coercive effort must be designed to influence outcomes in, or conduct with respect to" domaine réservé. They argued that having the effect of depriving the target state of control is insufficient. By contrast, the minority argued that when there is the effect above, the coercion condition is met. Concerning a hypothetical case in which a state's malicious cyber campaign is directed against cyber infrastructure owned by a particular ethnic group in another state, the minority regarded it as an intervention, while the majority took the opposite position. For the scenario to amount to an intervention, in the majority's view, it must be designed or intended to influence any outcome in the target state.[172]

Second, regarding a causal nexus to the effect on a target state, the majority of experts contended that indirect causation was enough, while the

minority required direct causation. They discussed a hypothetical example of the leaking of sensitive domestic intelligence records obtained through cyber espionage with the intention to cause a political crisis in a target state, then indirectly enforcing a policy favorable to an attacking state. The majority considered the case to be coercive, while the minority disagreed.[173]

Third, as regards whether there is a need for a target state to have knowledge that "it is being compelled into a particular course of action," the majority denied it, while the minority required it. Speaking of covert cyber operations to alter electronic ballot results in a target state, the majority contended that the target state is effectively forced into a particular outcome that would not otherwise have occurred, but the minority argued that the target must know of the intention from an attacking state.[174]

3.2.2 Case Studies

In respect of misinformation during the pandemic and the U.S. election of 2016, Schmitt and Milanović noted that "the point at which influence becomes coercion remains unsettled in international law, but some acts of misinformation would unambiguously qualify as prohibited intervention."[175] Schmitt goes further, arguing that Russian meddling operations that "feigned American citizenship and the hacking and subsequent release of private data" were in the legal grey zone, but might qualify as coercive, thereby amounting to intervention. As to whether the causation is direct or indirect, the second contentious point in the commentary to TM2 Rule 66, he evaluated that these operations indirectly impacted how voters choose candidates.[176] In terms of the third divided point above, a condition of knowledge, American voters were "unaware" of Russian operations while being exposed to them in 2016.[177] That does not hinder the coercion element being met, according to the majority view.

Schmitt and Milanović also discussed whether the WannaCry attack[178] could have amounted to prohibited intervention. They define coercion as "depriving the state of the *ability* to exercise such control or affecting the state's *will* to such an extent that its choices are no longer free ones."[179] They then draw the following skeptical conclusion:

> Although the attack was coercive in fact, WannaCry was not coercive vis-a-vis the domaine réservé of health care. Rather, the operation was designed to secure a ransom payment; albeit highly disruptive, it did not deprive the United Kingdom of the ability to exercise control over health care in the country, nor did it affect its will with regard to health care choices that North Korea wished to impose on the United Kingdom.[180]

In their assessment, the attack did not reach the required level of effects nor coercion regarding domaine réservé. First, as for the effects, it "directly affected the physical well-being of individuals in the United Kingdom,"[181] which was enough to make it qualify as a violation of British sovereignty due to the harm suffered,[182] but not for the purpose of rule of non-intervention. As stated in the extract above, the UK maintained the ability to exercise control over healthcare. Second, regarding coercion, there was an intention on the North Korean side to force the British government to do certain actions against its will: payment of ransom. However, this intention was not directed toward healthcare as domaine réservé.

The WannaCry attack might have been a relatively easy case to assess under TM2, as it neither involved any controversial points raised among TM2 experts nor met any of the conditions necessary to constitute prohibited intervention. Accordingly, the only avenue left for the UK to accuse North Korea would be a violation of its sovereignty for the harmful effects on patients. The British government, however, does not support the stand-alone sovereignty rule in TM2.

To conclude, what stands out in the majority view of TM2 experts is that an offender's clear intent to coerce must be directed toward the administration of *domaine reserve*, and the effort must be able to influence particular outcomes. In this regard, a gap remains with the minority view that the effect suffices. The required level of impact appears higher compared to the breach of sovereignty. A state ransomware attack[183] committed out of purely financial purposes (e.g., WannaCry) seems less likely to fulfill these requirements and to breach non-intervention rule, at least insofar as the majority view is concerned.

3.2.3 State Positions

(1) For

Although the position papers of most states refer to the non-intervention principle as customary international law, not all of them articulate their opinions clearly on how the element of coercion is fulfilled. Apart from the British government (referenced later), none of them explicitly support any of the three views proposed by the minority of TM2 experts: sufficiency of the effects, direct causation, and need for knowledge of coercive intent. On the contrary, at least nine states (Australia,[184] Costa Rica,[185] Denmark,[186] Estonia,[187] Finland,[188] Germany,[189] Norway,[190] Poland,[191] Switzerland[192]) appear to be in favor of the majority view regarding the first contentious point. For instance, Norway's statement relating to election meddling seems in line with the majority view: "carrying out cyber operations with the intent of altering election results in another State, for example by manipulating election systems or unduly influencing public opinion through the dissemination of confidential information obtained through cyber operations ('hack and leak'), would be in violation of the prohibition of intervention."[193] The New Zealand position is similar to these nine states, but a little more subtle, especially in the wording: "intention may in some circumstances be inferred from the effects of cyber activity."[194] Canada, Germany, Italy, and Japan express the need for further discussion or state practice concerning the elements.

(2) Against

The British government released its most recent position paper on how international law applies to cyber operations in 2022.[195] This provides a clue about how the UK might consider certain "disruptive cyber conduct" on "essential medical care" in the context of non-intervention. Raising the question of "whether disruptive cyber behaviours are coercive even where it might not be possible to point to a specific course of conduct which a State has been forced into or prevented from taking," the British Attorney General illustrated coercive intervention in the medical sector with the following scenarios.

- disruption of systems controlling emergency medical transport (e.g., telephone dispatchers)

- causing hospital computer systems to cease functioning
- disruption of supply chains for essential medicines and vaccines
- preventing the supply of power to housing, healthcare, education, civil administration and banking facilities and infrastructure

Combined with the statement that "coercion can be broader than … compelling [a State] into a specific act or omission," it initially appears as though a specific coercive intent on the offender's side need not be specified, and even state ransomware attacks with a merely financial purpose might be regarded by the UK as coercive intervention depending on the scale and severity. Should this be the case, the British view may be akin to the minority view of TM2 experts about the first point of disagreement.

3.2.4 Summary

It has been well established in physical domains that two elements need to be fulfilled for prohibited intervention to exist: domaine réservé and coercion. While no objection is voiced for treating cyber acts similarly, the element of coercion was more contentiously debated during the TM2 project and will thus be at issue in TM3. The question of election meddling, especially as influence operations, will be near the top of agenda, as it remains an unsettled issue. As the WannaCry case illustrates, a more cumbersome question is whether certain disruptive cyberattacks could be recognized as coercive enough when a specific intent to force a course of action or an outcome concerning domaine réservé against a target state's will is difficult to prove. The rule of non-intervention, including the coercion element, will definitely require further in-depth review for all states, not just for states like the UK that do not accept a stand-alone rule of sovereignty.

3.3 Due Diligence

Due diligence "has traditionally been invoked (and still is) in situations where it establishes the legal responsibility of a State in connection with the behaviour of private actors that cannot be attributed directly to the State."[196] In this regard, it is worth noting that in its well-known dictum in the *Corfu Channel* case, the ICJ affirmed "every State's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States."[197] As TM2 notes, the general principle of sovereignty imposes legal obligations to exercise due diligence to terminate harmful cyber activities emanating from a state's territory.[198]

3.3.1 TM1 & 2

(1) TM1

(a) Basic Rule

The due diligence principle is originally covered in Rule 5 in TM1, although the terminology used in its commentary is "due care" instead of "due diligence."[199]

TM1 Rule 5: Control of Cyber Infrastructure[200]

> A State shall not knowingly allow the cyber infrastructure located in its territory or under its exclusive governmental control to be used for acts that adversely and unlawfully affect other States.

TM1 experts reached no consensus on several points. The first is whether constructive knowledge ("should have known") is required when a state is "unaware of"[201] an offending cyber operation on its territory. No further detailed discussion on this point was held during TM1, probably due to the failure of TM1 experts to find any common ground at that time. The second problem is whether a state through which cyber operations are routed (the transit state) bears an obligation to act against a harmful cyber operation.[202] Here, the TM1 experts did not give any particular example. Overall, however, TM1 recognized the due diligence obligation as *lex lata* and an injured state's entitlement to the circumstances precluding wrongfulness such as countermeasures and the right of self-defense "[i]f a State fails to take appropriate steps."[203]

TM2 experts took over the review of the due diligence principle from TM1 experts. Consequently, Rules 6 and 7 in TM2 replaced TM1 Rule 5.

(b) Due Diligence and *Jus Ad Bellum*

As a substitute for the due diligence in the context of the *jus ad bellum*, TM1 experts discussed the "unwilling and unable" test. But TM1 did not create a black-letter rule for that purpose. Instead, the test was only covered in the commentary to TM1 Rule 13 on the right of self-defense against an armed attack.[204] Unlike the basic rule of due diligence in peacetime, an update on TM1 Rule 13 was tasked to the same TM1 experts for the purpose of TM2, and their consideration is still valid in renumbered Rule 71 of TM2.

(2) TM2

(a) Overview: TM2 Rules 6 and 7

TM2 experts upheld the TM1 stance that the due diligence obligation has *lex lata* status in the cyber context, which is in clear contrast to UN GGE Reports of 2013[205] and 2015,[206] both of which categorized it as a voluntary, non-binding norm.

TM2 created a dedicated chapter on due diligence and elaborated on requirements such as the threshold of harm and scope/character of the obligation. TM2 also provided solutions to pending issues in TM1, such as a transit state's obligation[207] and constructive knowledge.[208] With respect to the former, TM2 illustrated the obligation through an example of a fiber optic cable that is laid inside the territory or waters of the transit state and a botnet setup for malicious purposes.[209] But it seems as though the majority of TM2 experts are at least judging the existence of a due diligence obligation not by a categorical standard, but rather on the basis of conditions such as knowledge[210] or requisite harm.[211] Thus "the transit State" bears due diligence obligations on some occasions but not on others. Next, in respect to the latter issue, TM2 affirmed the constructive knowledge standard, citing Judge Alvarez's separate opinion in the ICJ *Corfu Channel* case, adding a caveat that "in international law generally, the standard is somewhat controversial."[212] TM2 suggests that the standard more likely applies when the exploited cyber infrastructure is

government-owned rather than private. This is the case with publicly known malware and vulnerabilities (e.g., Heartbleed vulnerability)[213] or DDoS attacks that are "generally always detected."[214]

TM2 Rule 6: Due Diligence (General Principle)[215]

> A State must exercise due diligence in not allowing its territory, or territory or cyber infrastructure under its governmental control, to be used for cyber operations that affect the rights of, and produce serious adverse consequences for, other States.

Regarding the threshold of harm, TM2 experts noted that for this rule to apply, there must be "cyber operations by a State that breach an international legal obligation owed to the target State" and that have "serious adverse consequences."[216] In the event of cyber operations perpetrated by non-state actors, there must be "serious adverse consequences" that "affect a right of the target State," as non-state actors do not violate international law *per se*.[217]

However, TM2 experts reached no consensus on where the threshold is set.[218] For example, "causing inconvenience, minor disruption, or negligible expense," such as "defacement of an official website of a State's Ministry of Sports that provides information on its national teams by hackers," does not suffice.[219] Conversely, the rule applies in the case of the defacement of "a website providing critical government services, as with ones used for payment of taxes, voting, or providing disaster relief guidance," that are "rendered unusable."[220] Similarly, as no physical harm is required in TM2's view, cyber operations aiming at "interference with the operation of critical infrastructure or a major impact on the economy" causing "the severe disruption of online banking, media, governmental functions, and business" suffice to meet the threshold.[221]

TM2 Rule 7: Compliance with the Due Diligence Principle[222]

> The principle of due diligence requires a state to take all measures that are feasible in the circumstances to put an end to cyber operations that affect a right of, and produce serious adverse consequences for, other states.

TM2 experts concluded that when the territorial state is unable to stop harmful cyber operations with all feasible measures, no violation results, even if the harm still exists. That is because, according to the Rule 7 commentary, the due diligence principle "is an obligation of conduct, not of result," and thus "does not demand that the territorial State always be successful in bringing to an end harmful uses of its territory."[223]

This point is a remarkable clarification that was not seen in TM1, but at the same time it raises a new question of consistency with other rules, specifically with the right of self-defense. As described below, the majority of TM1 experts appear to regard due diligence as an obligation of result, not just an obligation of conduct, in relation to *jus ad bellum*.

(b) Countermeasures for Non-Compliance of Due Diligence

The TM2 experts also updated the rules on countermeasures. The commentary to Rule 23 on the proportionality requirement, in particular, notes that "the proportionality of the countermeasure will be determined with respect

to the responsible State's omission, not vis-à-vis the severity and consequences of the cyber operations that the responsible State had a duty to terminate."[224] This is a reasonably understandable statement, since the purpose of countermeasures is to "induce a responsible State to comply with the legal obligations it owes an injured State" (Rule 21).[225] As discussed below in the section on responsive measures, a victim state of a malicious cyber campaign launched by a non-state actor must justify its trans-border cyber operations against them. But if the response is based on the territorial state's non-compliance with the due diligence rule, the scope of permissible counter-operations may be limited in nature.

(c) Due Diligence and *Jus Ad Bellum*

Regarding the use of force threshold, the TM1 experts all agreed that affording sanctuary (safe haven) to a terrorist group "may" breach the due diligence obligation despite not involving any use of force. In the majority's view, however, when the territorial state engages in more active involvement, it will qualify as a use of force. Providing malware and training to an organized group is such an example by analogy to the ICJ judgment in the *Nicaragua* case.[226] Furthermore, the majority of TM1 experts argued that there may be a use of force "in certain circumstances" when the territorial state provides sanctuary in conjunction with "substantial support or providing cyber defences for the non-State group."[227]

With regard to whether the right of self-defense may be invoked in response to non-compliance with the "unwilling and unable" test, the majority of TM1 experts concluded in the affirmative. In the commentary to the rule on self-defense against armed attack, they argued that self-defense is possible when the territorial state is not only *unwilling* but also *unable* (e.g., because it lacks the expertise or technology) to end non-state actor's cyber armed attack.[228] This proposition implies that the test of "unwilling and unable" in the *jus ad bellum* context is an obligation of result, unlike the obligation in a time of peace. It also suggests that a victim state's right of self-defense outweighs the sovereignty of the territorial state. A minority of TM1 experts objected to this majority view, arguing that a victim state must seek the consent of the territorial state or authorization by the UN Security Council if the armed attack is not attributable to the territorial state, although they recognized other legal options, such as the plea of necessity.[229] It is unfortunate that no precedent or reference is cited there from either side.

3.3.2 Case Studies

There are no reported cases in which due diligence was clearly invoked by a victim state in the cyber context. Although there is a case where an ISIS/ISIL hacker was killed in Syria,[230] that does not mean cyber activities in Syria led the U.S. and other states to invoke the "unwilling and unable" test.

3.3.3 State Positions

(1) Due Diligence in Peacetime

(a) For

While Australia (perhaps as a voluntary, non-binding norm), Canada, China,[231] Costa Rica, Denmark, Estonia, Finland, France, Germany, Ireland, Italy, Japan,

the Netherlands, Norway, Poland, Romania, Sweden and Switzerland are supportive of TM2's basic stance on the due diligence obligation, it is uncertain whether their support is extended to *jus ad bellum*, as is the case with the French position.

(b) Against

The U.S. practice described above regarding the right of self-defense does not necessarily mean it approves of how the TM2 experts understood due diligence in peacetime. On the contrary, the U.S. keeps denying the legally binding character of the due diligence principle due to the lack of state practice and *opinio juris* for that purpose.[232] New Zealand, Israel, and the UK adopt the same stance.[233]

(c) Silent or Neutral

Brazil, Czech Republic, Iran, Kazakhstan, Kenya, Pakistan and Russia do not mention due diligence in their papers, and Singapore takes a neutral stance by stating that there is a need for clarity on the obligation's scope and practical applications.[234]

(2) Test of "Unwilling and Unable" during Armed Conflict

Few states refer to this concept in their position papers, the most important being France and the U.S.

(a) For

The U.S. supports the right of self-defense by a victim state when the "unwilling and unable" test is fulfilled. In its view, a victim state of a cyber armed attack "generally must make a reasonable, good faith effort to seek the territorial State's consent" first, but "if the territorial State is unwilling or unable to stop or prevent the actual or imminent armed attack launched in or through cyberspace," then the state may use force in self-defense without consent.[235] The U.S. invoked the doctrine during a series of campaigns against ISIS/ISIL in Syria, with the support of Australia[236] and several other states.[237] Assuming that these states uphold the same approach in the cyber domain, the following states are supportive of the "unwilling or unable" test: Australia, Belgium (implicitly), Canada, Czech Republic, Denmark, Germany, Iran (implicitly), Israel, the Netherlands, Norway, Russia, South Africa (implicitly), Turkey, the UK and the U.S.

(b) Against

France unequivocally opposed the TM1 experts' majority view on "unwilling and unable" in self-defense, stating that "[t]he fact that a State does not take all reasonable measures to stop wrongful acts against other States perpetrated from its territory by non-State actors, or is incapable of preventing them, cannot constitute an exception to the prohibition of the use of force."[238] Other states that are known to reject the test in the non-cyber context are Brazil, Cuba, Ecuador, Mexico, Syria and Venezuela.[239]

3.3.4 Summary

TM1 and TM2 both affirmed the *lex lata* status of the due diligence obligation. TM2 also clarified the obligation's scope of application, especially regarding two issues that TM1 left unresolved: constructive knowledge ("should have known") and transit state. As for the responsibility of a territorial state

through which an armed attack is launched, the majority of TM1 experts supported the "unwilling and unable" test in the commentary to rule on the right of self-defense, thereby granting the right of a victim state to extend its defensive measures to the territorial state should the latter fail to end the ongoing armed attack. Both the due diligence obligation and the "unwilling and unable" test have been supported by some states in their position papers or in armed conflicts that were waged in the physical domain. Conversely, the UN cyber GGE reports deem due diligence a voluntary, non-binding norm due to the lack of consensus. The validity of black-letter rules and detailed interpretative points in the TM1 and TM2 commentaries will be tested down the road in the light of pertinent cyber incidents in which the due diligence is invoked by an injured state and other interested parties.

3.4 Collective Countermeasures

Under the ILC Articles on Responsibility of States for Internationally Wrongful Acts ('ARSIWA'), countermeasures are listed as one of the six circumstances to be applied to any international wrongful act, and they provide a justification or excuse for non-performance while the circumstance in question subsists.[240] Article 48 of ARSIWA, on "Invocation of responsibility by a State other than an injured State," focuses on the demand of "cessation of the internationally wrongful act, and assurances, and guarantees of non-repetition" in case of violation both owed to a group of States, and owed to the international community as a whole (para. 2 (a)(b)). It does not include countermeasures by a non-injured state. Part 3, chapter II, which includes "measures taken by States other than an injured State" simply describes "legal measures,"[241] which can in theory include countermeasures. The legal possibility of taking countermeasures by non-injured states is not covered in either place due to a perception that, in the view of ILC, they are controversial and supported only by embryonic practice.[242] The ILC also suggested that "[a]t present there appears to be no clearly recognized entitlement of States referred to in Article 48 to take countermeasures in the collective interest," due to state practice being sparse and involving a limited number of states.[243] Nevertheless, some commentators consider the matter to be left open, and Article 54 of ARSIWA does not exclude the option of collective countermeasures in cases involving the violation of at least obligations *erga omnes*,[244] and procedurally speaking if the Security Council fails to impose mandatory sanctions under UN Charter Chapter VII.[245]

3.4.1 TM1 & 2

(1) TM1

TM1 did not address the question of collective countermeasures in the commentary to Rule on countermeasures.[246]

(2) TM2

TM2 reached the same negative conclusions as ILC did, not approving collective countermeasures as customary international law and not creating a black-letter rule due to the lack of consensus among the experts, as shown below.[247]

TM2 Rule 24: States Entitled to Take Countermeasures[248]

'Only an injured State may engage in countermeasures, whether cyber in nature or not.'

The phrase "only an injured State" suggests that collective countermeasures are not permitted under the *lex lata*, although a few of the TM2 experts were in favor of the concept, noting that collective countermeasures are possible upon request from an injured state.[249] They cited several supportive state practices that the ILC described as "limited and embryonic" at the time of the ILC work. The states invoked some of these precedents involving collective countermeasures regarding questions in cases related to genocide, apartheid, and humanitarian crises in Kosovo,[250] while other cases were instead asserted by states concerned as justifying suspension of a treaty due to a fundamental change of circumstances.[251] However, despite the rejection of the concept, some of the TM2 experts supported the right to provide certain types of assistance to an injured state, such as providing "guidance on how to conduct a hack-back qualifying as a countermeasure, or shar[ing] information regarding vulnerabilities in the responsible State's cyber infrastructure."[252]

3.4.2 Case Studies

There have not been any publicly reported cases of collective cyber countermeasures.

Covering a series of cyber operations discovered in 2010 to 2012 in Iran (e.g., Stuxnet, Flame, Duqu), Roscini assessed that "it is not controversial that Iran has breached Security Council resolutions requiring it to suspend all uranium enrichment-related activities," and "Article 25 of the UN Charter is an *erga omnes partes* obligation owed to all other UN Member States." But even assuming that "lawful measures" in Article 54 include countermeasures, the U.S. "was not entitled to adopt countermeasures, including cyber operations, under Article 54," because the Security Council has already adopted mandatory sanctions.[253] Therefore, these cyber operations targeting Iran do not constitute a precedent for collective countermeasures.

Likewise, when the U.S. Cyber Command engaged in "Defend Forward" cyber operations against Iran in June and September 2019, following Iranian attacks on both the U.S. targets and non-U.S. flagged tankers in June 2019 and Saudi Arabia's oil facilities in September 2019, the U.S. government did not describe its actions as collective countermeasures, nor did other victim states request them.[254] Moreover, the ongoing hostile relationship between the U.S. and Iran complicates the legal characterization of arbitrarily selected episodes of the campaign between them.[255]

With regard to counter-ransomware operations, Schmitt presents three pillars of TM2 rules as justifying the operations: sovereignty as a rule, due diligence, and collective countermeasures.[256] His proposal makes sense, especially when ransomware attacks are conducted by non-state actors that are not attributable to a state. In this circumstance, a countermeasure against a non-state actor is not permissible under international law. The rule of due diligence then gives a victim state a legal justification to launch trans-border cyber operations in the name of countermeasures against the territorial state. Focusing on cyber-incapable victim states, Schmitt argues that if it were not for an option of collective countermeasures, such a restrictive interpretation "would leave many states *de facto* defenseless in the face of hostile cyber

operations."[257] The U.S.[258] or Canada[259] reportedly engaged in such counter-ransomware operations in order to take down the cyber infrastructure utilized by the foreign criminal group and to thwart further attacks on entities located in the territories of both countries. However, they have explained neither how they legally evaluated the malicious actions nor the legal basis for their measures in cyberspace.

3.4.3 State Positions

(1) For

Interest in the notion of cyber collective countermeasures has been sparked since 2019, when then-Estonian President Kersti Kaljulaid proposed it in her speech during CyCon, the annual NATO CCDCOE conference.[260] As for state position papers (in addition to Estonia), Costa Rica,[261] Denmark,[262] Ireland[263] and New Zealand[264] are favorable to collective countermeasures. Costa Rica, Denmark and Ireland, in particular, refer to "obligations of an *erga omnes*" nature, an "obligation owed to the international community as a whole," and "peremptory norms," respectively, as examples of where the violation of these obligations may justify collective countermeasures. Despite slightly different terminology being used in their position papers, these three states seem to be on the same page concerning Article 48 of ARSIWA. Costa Rica is the clearest example, specifically citing that article. The phrase "States which are not directly injured" in Estonia's position can be interpreted as meaning almost the same.

(2) Against

Canada[265] is dismissive of the customary law status of collective countermeasures and, hence, their permissibility. In view of the fact that it supports TM2's basic rules of sovereignty and due diligence, a potential explanation for the counter-ransomware operations by the Canadian Communications Security Establishment (CSE) might be as solo- or joint countermeasures with the U.S., not as collective ones in the interest of other victim states. France also rejects collective countermeasures, noting that the state "rules out the possibility of France taking such [collective counter] measures in response to an infringement of another State's rights."[266]

(3) No Position

Most other states endorse countermeasures as a legally viable option available to an injured state, but they do not refer to the question of collective countermeasures in their position papers. Brazil stands out in terms of expressing doubt about the customary character of collective countermeasures.[267] If the U.S. maintains its previously declared rejection of the *lex lata* status on both sovereignty as a rule and due diligence in cyberspace, it is unlikely to accept the permissibility of collective countermeasures. If so, American assistance to states that fall victim to severe cyberattacks would be justified differently, regardless of how the victim states interpret the U.S. actions.

3.4.4 Summary

The question of cyber collective countermeasure appeared in TM2 for the first time, but TM2 experts were split over whether their permissibility has obtained customary law status. The majority view was negative, like the ILC was regarding ARSIWA. Conversely, some scholars have advocated for collective

countermeasures both in general and in the cyber context, and some states are proactive in supporting cyber collective countermeasures. Further in-depth review must continue pending the potential evolvement of the law in this area.

3.5 Necessity

Like the countermeasures above, the state of necessity is one of the six circumstances precluding wrongfulness listed in ARSIWA. Article 25 of ARSIWA provides that "necessity may not be invoked by a State … unless the act (a) is the only means for the State to safeguard an essential interest against a grave and imminent peril, and (b) does not seriously impar an essential interest of the State or States toward which the obligation exists, or of the international community as a whole."[268] The commentary notes that "there is substantial authority in support of the existence of [it] as a circumstance precluding wrongfulness. It has been invoked by States and has been dealt with by a number of international tribunals."[269]

3.5.1 TM1 & 2

(1) TM1

TM1 addressed the plea of necessity very briefly in the commentary to Rule 9 on countermeasures, but it did not articulate a black-letter rule on the subject.[270] TM1 appears to be more in line with Article 25 of ARSIWA than TM2, as it includes within its scope an essential interest of international community as a whole.[271] As protective measures based on necessity, however, TM1 lists only the examples of "temporarily shutting off certain cyber infrastructure," without describing the location of this effected infrastructure and "counter-hacking."[272]

(2) TM2

TM2 Rule 26 below and its commentary generally build on Article 25 of ARSIWA and its commentary.

TM2 Rule 26: Necessity[273]

> A State may act pursuant to the plea of necessity in response to acts that present a grave and imminent peril, whether cyber in nature or not, to an essential interest when doing so is the sole means of safeguarding it.

The plea of necessity may be invoked in the face of a state-launched cyber operation, a non-state actor operation, or a cyber operation of unknown origin. TM2's commentary affirms the plea's *lex lata* status and its application to the cyber context, despite its precise nature and scope still being at issue.[274]

(a) "An Essential Interest"

TM2 listed some examples of a cyber operation placing "an essential interest" being in grave and imminent peril, as follows: debilitating the state's banking system, causing a dramatic loss of confidence in its stock market, grounding flights nation-wide, halting all rail traffic, stopping national pension and other social benefits, altering national health records in a manner endangering the health of the population, causing a major environmental disaster, shutting

down a large electrical grid, seriously disrupting the national food distribution network, or shutting down the integrated air defense system.[275] The TM2 Director added an operation targeting blood banks during a natural disaster with consequences of significant loss of life to the list.[276]

Particularly when critical infrastructure is targeted by cyberattacks from an unknown source, resulting in the disruption of its operation, the consequence may be identified as an essential interest in grave and imminent peril. Nevertheless, TM2 adds the caveat that "a State's unilateral description of infrastructure as critical [is not] determinative of the issue" of whether it is an "essential interest."[277]

(b) Lack of Connection to a Prior Wrongful Act of a State

The state of necessity is "not dependent on the prior unlawful conduct of another State."[278] With respect to cyber operations that are launched by a non-state actor and meet other conditions for the state of necessity, TM2 approves the invocation of necessity "in circumstances where no State is responsible for the operation"[279] unless they "affect the essential interests of other States."[280] Thus, the state of necessity in this situation raises doubts about the relevance of the principle of due diligence. As long as the territorial state from which non-state actors stage an attack complies with the requirements of due diligence, countermeasures are not permitted.

The question then arises as to whether the victim state in the same situation may nevertheless be entitled to invoke the plea of necessity because of its essential interest being endangered. From a literal reading of the commentary to necessity, TM2's answer appears positive. Even if the sovereignty of the territorial state is breached by necessity measures, the wrongfulness can be precluded on the condition that the essential interest of the territorial state is unaffected. In that sense, it seems as though the state of necessity in TM2 may diminish the role played by the principle of due diligence. Under the due diligence principle, countermeasures by another state are prohibited when a genuinely willing territorial state is unable to terminate trans-border harmful cyber operations within its territory, because due diligence is an obligation of conduct (not of result), meaning that the territorial state is not required to put an end to malicious cyber operations by non-state actors.[281] However, the state of necessity may be invoked in this situation after all. The principle of due diligence will be even more meaningless if a state invoking necessity is not obliged to take into consideration the extent to which the territorial state is exercising due diligence as an urgent matter, since in theory necessity and due diligence are expected to function in completely different conditions.

Lastly, although not stated clearly in TM2, the state of necessity can be subject to subsequent control by a third party,[282] similar to how countermeasures are taken at their own risk and a state may be held accountable for taking such countermeasures with mistaken attribution.[283] Therefore, if necessity is invoked after misjudging the essential interests concerned, the invoking state will be responsible for its illegitimate measures.

(c) Contentious Issues in TM2

TM2 experts reached consensus on all but three points. The first is whether forcible measures can be subject to the plea of necessity. The same question has been debated with respect to countermeasures, and long before cyber technology emerged. "Some of the Experts" rejected the invocation of necessity unless force is employed as the right of self-defense or authorized by the

UN Security Council. "The other" experts supported the ability to invoke necessity in the event of an unlawful use of force where "the only effective response is a use of force for a victim State."[284]

The second contentious issue is the scope of "essential interest." The majority of TM2 experts were of the view that "only interests of States are protected by operation of the plea of necessity in the present state of the law," while acknowledging "extreme cases" where the plea may be invoked to serve the interest of "international community as a whole."[285] In this regard, the majority's view seems more restrained than the ILC's conclusion in ARSIWA that placed the international community as a whole within the scope of the plea.[286] A wider interpretation of protective interests implies the potential case of "several States acting together unilaterally" for the plea of necessity.[287]

The third point of disagreement concerns a cyber-specific scenario. TM2 experts were split over "whether the possibility of cooperation with other States or with international organisations" disentitles a state to invoke the plea. TM2 experts discussed a hypothetical scenario where a State A is hit by a cyber operation launched from cyber infrastructure located in a friendly State B. State B has a CERT that is highly cyber-capable. The majority, following the ILC approach, argued that State A "would have to, if time permits and it is feasible to do so otherwise in the circumstances, solicit the assistance of the CERT" first. The minority opposed that position, noting that "the notion of alternative means only refers to means that are within the exclusive control of the State claiming necessity."[288]

3.5.2 Case Studies

Because of the lack of reported precedents in the cyber domain,[289] envisaging what a cyber operation based on the plea of necessity will look like is not easy.

With regard to counter-ransomware operations discussed above, one may ask whether the plea of necessity is a better fit than state countermeasures for explaining their legal basis. In this respect, one condition may be recalled for invoking the plea of necessity: the peril will not yet have occurred.[290] In other words, to cite the TM2 experts, a state resorting to action based on the plea of necessity need not face a peril that has materialized before it takes action.[291] TM2 experts agreed that the plea applies equally when the cyber operations in question are underway and the harm is manifesting.[292] Thus, in terms of the harm in question, the plea of necessity may be invoked for cyber incidents where countermeasures appear to be a more likely justification due to harm already being suffered as a result (presumably) of a breach of due diligence by the territorial state. However, in the case of cyber operations launched by non-state actors, where the invocation of countermeasures is unavailable due to the non-eligibility of non-state actors as an addressee of countermeasures, the state of necessity may be the only option left for a victim state to protect its essential interest from more severe effects to come.

3.5.3 State Positions

(1) For

Eleven States recognize the applicability of the plea of necessity in the cyber context. Most references to necessity are very brief,[293] however, with the exception of Germany,[294] the Netherlands[295] and Norway.[296] The Netherlands provides examples of necessity, including a scenario where virtually the entire

internet is rendered inaccessible or severe shock is caused to financial markets. Norway provides unique insight into a prospective case in which the state of necessity is expected to apply: "if infrastructure in a third country is used in an internationally wrongful cyber operation, the injured State may under certain conditions launch a cyber operation to destroy or disrupt the internationally wrongful cyber operation, even if this violates the territorial sovereignty of the third State."[297] With this sentence, Norway shows its view that the state of necessity can be triggered not just by non-state actors, but also by the unlawful cyber operations of a state, which at first glance contradicts the TM2 view that it is "not dependent on the prior unlawful conduct of another State."[298] Moreover, Norway implies that the principle of due diligence does not come into play in such a circumstance, meaning that irrespective of whether the third State is in conformity with due diligence, the sovereignty of the third state will be violated.

(2) Against

No state explicitly opposes the applicability of the plea of necessity in cyberspace.

(3) No Position

The position papers of Australia, Brazil, Canada, China, Czech Republic, Denmark, Estonia, Kazakhstan, Kenya, New Zealand, Pakistan, Poland, Romania, Russia, Singapore and the UK make no reference to the plea of necessity.

3.5.4 Summary

Although there have not been any reported cases of a state invoking necessity in the cyber context, TM2 affirmed the customary status of necessity. Eleven countries support that conclusion. TM2 mostly followed the conditions laid down in ARSIWA, but unlike ARSIWA, most of the TM2 experts excluded the interests of the international community as a whole from necessity's scope of application.

Under the plea of necessity, a victim state may be entitled to take measures to safeguard its essential interests in the face of harmful cyber incidents unless those measures affect the essential interests of other states.

Necessity-based measures are permissible regardless of whether due diligence is complied with by the territorial state from which harmful operations are conducted. In this case, the sovereignty of the territorial state may be violated to the extent that the conditions for the plea of necessity are fulfilled.

3.6 Extraterritorial Jurisdiction

The terms "extraterritoriality" and "extraterritorial jurisdiction" refer to the competence of a state to make, apply, and enforce rules of conduct with respect to persons, property or events beyond its territory. Such competence may be exercised by way of prescription, adjudication or enforcement. Enforcement jurisdiction refers to a state's authority to ensure compliance with its laws.[299]

3.6.1 TM1 & 2

(1) TM1

TM1 addresses extraterritorial jurisdiction only in relation to enforcement jurisdiction by the flag states or states of registration over cyber infrastructure.

For instance, "a State may not exercise jurisdiction over cyber infrastructure aboard a commercial drone registered in another State that is operating in international airspace by taking control of that drone."[300]

(2) TM2

TM2 Rule 11: Extraterritorial Enforcement Jurisdiction[301]

> A State may only exercise extraterritorial enforcement jurisdiction in relation to persons, objects, and cyber activities on the basis of:
> (a) a specific allocation of authority under international law; or
> (b) valid consent by a foreign government to exercise jurisdiction on its territory.

(a) Terminology

The commentary to Rule 11 indicates a shared understanding among TM2 experts that enforcement jurisdiction is binary, either territorial (legal) or extraterritorial (illegal), unless otherwise specified by both (a) and (b) of black-letter Rule 11 above. The terminology in TM2 may cause confusion, but there is no such thing as lawful extraterritorial enforcement jurisdiction without a specific legal basis.[302] State B accessing servers located in State A may appears to be a trans-border operation, thus constituting extraterritorial jurisdiction, but in legal terms it is territorial exercise of jurisdiction due to the public accessibility of the servers.[303] Likewise, accessing data in closed online forums, chat channels, private Internet hosting services, or the so-called "dark web" in another state are also a territorial exercise of enforcement jurisdiction according to categorization by TM2.

Another illustrative example in TM2 is a case where one state's agent accesses a closed online forum hosted on servers in another state using credentials they obtained under false pretenses. This access is territorial enforcement jurisdiction, since the data is "meant to be accessible to one or more users from the State."[304] It becomes extraterritorial when the data in question is not meant to be accessible despite being connected to the internet.[305]

(b) Contentious Issue in TM2

TM2 experts were "evenly split" over an issue of indirect access to data through an internet service provider. In this hypothetical scenario, where law enforcement is seeking data that is not publicly available (e.g., subscriber or traffic information) some experts regarded it as unlawful extraterritorial jurisdiction based on the accessibility standard used for the discussion on the dark web. Other experts suggested that a mere request does not amount to extraterritorial jurisdiction and is thus lawful unless the request is followed by some kind of coercion to ensure compliance.[306]

3.6.2 Case Studies

(1) Tidal Case in Norway

State practice concerning remote cyber operations for criminal investigation purposes is getting richer, but it is still not uniform and even worse, not always admitted by the investigating state.[307] That said, some of new cases that took place after the publication of TM2 may fall within "territorial" enforcement jurisdiction proposed by TM2.

In the *Tidal* case at the Norwegian Supreme Court (2019),[308] for example, which involved computer fraud, the Norwegian law enforcement authorities, Økokrim (Norwegian National Authority for Investigation and Prosecution of Economic and Environmental Crime) downloaded data from a server belonging to Amazon Web Services in the U.S. using access credentials gained from the company. The Supreme Court of Norway upheld the legality of the search, stating that the coercive measure was initiated on Norwegian soil, against a Norwegian company, with offices in Norway, in the form of an order to the company to provide the information necessary for Økokrim to access the data, and "the search only involve[d] access to information the company itself has stored." While "the data remains on the server abroad," the court added that "no changes are made to the stored information, for instance in the form of deletion of encryption." According to the Court, nothing in the Budapest Convention on Cybercrime directly addresses a measure like the one in the *Tidal* case,[309] nor is there any customary international law in this area.[310] The Court thus held that "in a situation like the one at hand," it could find "that the search will affect another state to an extent that it constitutes a violation of the principle of sovereignty."[311]

The Norwegian Supreme Court also investigated the trends in neighboring countries, including Denmark (below) and Sweden, together with regional organizations in Europe. A dominant view in Sweden at that time disfavored a search for data stored abroad. However, the Norwegian Supreme Court seemed more sympathetic to the view presented in a Swedish Official Report on secret data reading, which questions the territorial principle preventing the remote access of data abroad, considering the storage site being both irrelevant and unknown to the user and, hence, concluding that "it is hard to see why the storage place in these cases should determine the executive jurisdiction issue."[312]

(2) Danish Supreme Court Order U 2012.2614 H

The Danish case cited in the Norwegian *Tidal* case concerned the Danish police reading the defendant's profiles on both Facebook and Messenger in October 2010, at which time the defendant resided in Canada. The Danish police accessed them as part of a criminal investigation into a drug-related crime subject to Danish criminal jurisdiction. The search was conducted in a Danish police office using credentials obtained through telephone intercepts and did not involve assistance or cooperation either from service providers such as Facebook and Messenger or from the local authorities in the U.S., Luxembourg or Canada. In May 2012, the Supreme Court of Denmark approved the police actions as duly authorized under Danish domestic legislation.[313]

The Norwegian and Danish cases both concern direct remote access to data abroad by law enforcement authorities. In both cases, the data in question seems to meet the TM2 public accessibility test. If that is not the case, the data search in the Norwegian case would be valid as extraterritorial exercise jurisdiction, since a data holder was present in the territory of Norway at the time when the search was conducted. The TM2 commentary states that "the State may exercise enforcement jurisdiction over the individuals or private entities themselves if they are located in the State, based on, for instance, the failure to cooperate with authorities."[314] While the Danish authorities conducted the search without his presence in Denmark, the Norwegian Supreme Court did not find any difference between the two cases.

(3) Skype Communications Case in Belgium

A Belgian case in 2019 regarding a production order issued to Skype Communications seems more controversial. The Belgian Court of Cassation reasoned that despite the lack of a branch, any infrastructure, or physical presence in Belgium:

> a provider [of an electronic communications service] is sometimes subject to Belgian legislation because of the mere fact of its active participation in economic life in Belgium. The cooperation obligation [to provide the requested information and provide technical assistance with the wiretapping measures] does not require intervention by the Belgian judicial authorities abroad. Consequently, the investigating magistrate is not obliged to make a request for mutual legal assistance to Luxemburg, where the provider has its establishment or infrastructure.[315]

The ruling stands in sharp contrast to the view of TM2, leading to the opposite conclusion concerning whether to view a request for extraterritorial data as the legitimate exercise of territorial jurisdiction or the illegitimate exercise of extraterritorial jurisdiction. With respect to directly requesting private foreign hosting service providers to obtain extraterritorial data (subscriber or traffic information) without a request for mutual legal assistance to a foreign state, the TM2 experts all denied the existence of any legal obligation for the providers to obey the request. Especially given that the data in question is not publicly available, some TM2 experts contended that "gaining access to it requires either a specific allocation of authority under international law or consent of the State enjoying enforcement jurisdiction over the data sought." Other TM2 experts affirmed the legality of a mere request to the provider "that is not accompanied by compulsion to comply on the part of the requesting state, thus not ris[ing] to the level of interference with the exclusive right of the other State to exercise enforcement jurisdiction on its territory."[316] In the Belgian case, the requested data was user data and an order to the provider was more than a mere request; accordingly, it would have been regarded as an impermissible exercise of extraterritorial jurisdiction under TM2 standards.[317]

(4) Take-down Operations in Third States beyond the Conflict Zone

Categories of enforcement jurisdiction other than remote operations for the purpose of criminal investigation may also fall within TM2 Rule 11 to the extent that it is conducted by government agents with domestic authorization. In particular, the standard of whether data is "meant to be accessible to one or more users from the State" may transform the legal character of counter-ISIS/ISIL operations that were conducted in third states (i.e., other than Iraq and Syria). The U.S. and Australia reportedly felt the need to take down cyber infrastructure used by ISIS/ISIL in third states, because ISIS/ISIL media nodes were dispersed globally. Legal rights and duties between the U.S. and Australia on one side and the third states on the other are governed primarily by peacetime norms, despite the operations being an extension of non-international armed conflicts fought in Iraq and Syria. The public accessibility standard described above, if applicable in this circumstance, may make it easier for the U.S. and Australia to legally justify the operations. The operations would have been considered lawful territorial jurisdiction despite being trans-border. Having said that, if the operations in question involved more than a negligible

effect and caused damage to or a loss of functionality of the target cyber infrastructure used by ISIS/ISIL, the operations would violate the sovereignty of the third states and thus require separate legal justification. In this regard, U.S. experts note that a state "is not precluded from taking action against ISIS's cyber facilities in other states, even without the consent of the host state, unless doing so constitutes a prohibited intervention or use of force."[318] Given the lack of any official announcement, it is uncertain how exactly the U.S.[319] and Australia[320] would characterize their operations.

3.6.3 State Positions

(1) For

Canada has demonstrated its clear view that "cyber activities carried out remotely from within Canada with negligible effects in a foreign State do not involve an extraterritorial exercise of enforcement jurisdiction by Canada."[321] This approach seems to be in harmony with TM2. The Netherlands, although clearly supportive of remote searches in cyberspace given its investigative practices,[322] is not as vocal as Canada in its position paper.[323]

(2) Silent or Neutral

Most position papers do not refer to extraterritorial enforcement jurisdiction. Germany[324] and New Zealand[325] raise the issue briefly, and the latter underlines a need to discuss it further in an appropriate multilateral forum.

(3) International Law-Making at International Organizations

Recent law-making trends in multilateral settings also deserve to be noted. In May 2022, the Second Additional Protocol to the Cybercrime Convention on Enhanced Co-operation and Disclosure of Electronic Evidence (CETS No. 224) was opened for signature.[326] Under Article 7 of the Protocol, a party is entitled "to issue an order to be submitted directly to a service provider in the territory of another Party, in order to obtain the disclosure of specified, stored subscriber information in that service provider's possession or control." A leading commentator, however, believes the Protocol is "unlikely to command the support of all States Partis to the Budapest Convention."[327]

Negotiations at the UN on a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes are also underway. The modalities of investigation of the criminal offenses listed in the draft convention circulated in the sixth session of the Ad Hoc Committee in August–September 2023 are limited to mutual legal assistance in the traditional sense.[328] The impact that these trends will have on the question of extraterritorial enforcement jurisdiction in cyberspace remains to be seen.

3.6.4 Summary

According to the TM2 terminology, the extent of "territorial" enforcement jurisdiction is wider than one may think, encompassing trans-border access to servers in another country that is consistent with the public accessibility standard. Conversely, extraterritorial enforcement jurisdiction is unlawful unless it has a specific legal basis in international law. As for a state request to foreign service providers to produce data stored in another country that does not go through the law enforcement authorities in that state, TM2 experts expressed diverse views. The most extreme view was that a mere request amounts to

extraterritorial jurisdiction and is therefore unlawful. National practice contradictory to this view exists and should be noted. The number of state position papers mentioning the topic is very small, but Canada highlights the point most accurately and in conformity with TM2.

3.7 IHL-Regulated Cyber Operations

Finally, this report examines the notion of attack under IHL. As described below, the notion is used in many provisions in international treaties and thus triggers the application of various IHL rules.

3.7.1 TM1 & 2

(1) TM1

TM1 Rule 30:[329]
Definition of Cyber Attack

> A cyber attack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects.

TM1 Rule 30 is partly derived from Article 49 (1) of API, which provides that "'[a]ttacks' means acts of violence against the adversary, whether in offence or in defence."[330] The remaining part of Rule 30 is built on "numerous Articles" of API, such as Article 51(1) on the protection of civilians, 51(5)(b), 57(2)(a)(iii), and 57(2)(b) on proportionality, 35(3) and 55(1) on protection of the environment, and 56(1) on the protection of works and installations containing dangerous forces. According to TM1 experts, those rules all contain a common element for the definition of attack: the consequential harm.

(2) TM2

Rule 30 is renumbered Rule 92 in TM2, with a little update in the commentary. The black-letter rule of TM2 92 is exactly the same as TM1 Rule 30.

TM2 Rule 92:
Definition of cyber attack[331]

> A cyber attack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects.

(a) Protective Scope

With regard to what determines "attack" under IHL, TM1 experts agreed that the key criterion is the consequence of a party to a conflict's actions.[332] Thus, a cyber operation that causes only *de minimus* damage or destruction does not constitute "attack" under IHL.[333] Beyond that, however, the TM1 experts expressed diverse views concerning the level of consequence required to qualify as "attack."

On the other hand, there was consensus among TM1 experts concerning the idea that an operation affecting data is an "attack" whenever that operation foreseeably results in the required consequence (whatever that may be).[334]

(b) Interference with Functionality

TM1 experts were divided over the issue of interference with functionality. The majority considered actions requiring physical components to be replaced as an attack.[335] The experts also discussed a hypothetical case of cyberattacks against the computer-based control system of an electrical distribution grid. When the control system or vital components of the grid must be restored for the grid to be operational again, the majority considered the operation an "attack." Other experts went further, extending "attack" to cases in which recovery requires the reinstallation of an operating system or particular data.[336] Moreover, in the case of "the loss of usability of cyber infrastructure," where required work is only data restoration—not the replacement or reinstallation described above—"a few Experts" suggested such an operation could still amount to "attack."[337]

The ICRC is known for adopting the same view as the minority of TM1 experts. Relying on the term "neutralization" in Article 52(2) of API, the ICRC considers that "attack" includes "operations designed to impair the functioning of objects (i.e. neutralize them) without causing physical damage or destruction." The ICRC bases its argument on the object and purpose of the rules on the conduct of hostilities, which is to ensure the protection of the civilian population and civilian objects against the effects of hostilities.[338]

(c) Large-Scale Adverse Consequences

TM1 experts were also split over the issue of how to view large-scale adverse consequences (e.g., disrupting all email communications throughout the country). The majority did not view such consequences as an attack, while the minority predicted that the "international community would generally regard them as attack."[339]

3.7.2 Case Studies

According to Deputy Chairman Victor Zhora of the State Service of Special Communications and Information Protection of Ukraine, Russian cyber operations have shifted from destructive ones in the early phase of the invasion to cyber espionage or efforts to support kinetic actions.[340] In light of the focus in the Tallinn Manuals on cyber-to-cyber operations, *sensu stricto*,[341] what needs to be examined here are episodes in which cyber-means are exclusively used. NotPetya may be worthy of assessment in this respect. It is widely known as the most devastating cyberattack at the time,[342] with at least four hospitals reported to have fallen victim in Kiev alone.[343] Although information on the resulting consequences is unknown, worsened patient conditions equivalent to those caused by kinetic attacks may well qualify under the TM1 standard as amounting to an "attack" under IHL. TM1 experts note that "any reasonably foreseeable consequential damage, destruction, injury, or death" is encompassed under "attack,"[344] yet it is uncertain whether they intended to go so far as to include "the violent tertiary effects on human life" resulting from attacks on cyber infrastructure.[345]

If the affected systems had required the replacement of physical components, at least the majority of TM1 experts would recognize it as amounting to an "attack."[346] Taking account of the consequences that resulted in a Danish company, Maersk, which required more than reinstallation of the system for recovery to the normalcy,[347] and assuming the same level of effects that occurred in Ukraine, NotPetya could be regarded as an "attack" in accordance with the minority view of TM1 experts, along with the nine states in (2) below

and the ICRC. The same arguments apply to other related cyber operations in Ukraine.[348]

In August 2023, the International Criminal Court (ICC) Prosecutor presented his view that the ICC will scrutinize war crimes enabled by cyber-means,[349] and the Ukrainian government is collecting evidence of Russian cyber-war crimes for that purpose.[350] Consequently, we may someday see a prosecution of cyber war crimes committed in the Russo–Ukrainian War.

3.7.3 State Positions

(1) View that "Attack" Excludes Loss of Functionality

Israel claims that "the mere loss or impairment of functionality to infrastructure would be insufficient in this regard, and no other specific rule to the contrary has evolved in the cyber domain."[351]

(2) View that "Attack" Encompasses Loss of Functionality

States that support an expansive view of "attack," one that includes loss of functionality, include Canada, Costa Rica, France, Germany, Ireland, Italy, Japan, New Zealand and Pakistan. Of these nine states, the views of Costa Rica, France and Ireland resemble the ICRC position. Ireland is the clearest example, as it cites the ICRC's view in its position paper.[352] Costa Rica suggests the most expansive view, noting that it "understands damage to include the disabling – temporary or permanent, reversible or not – of the targeted computer, system, or network."[353] Interestingly, it lists ransomware, "despite being temporary and reversible," as an example of "attack." France straightforwardly rejects the definition adopted by TM1 experts, arguing that "a cyberoperation is an attack where the targeted equipment or systems no longer provide the service for which they were implemented, whether temporarily or permanently, reversibly or not. If the effects are temporary and/or reversible, the attack is characterized where action by the adversary is necessary to restore the infrastructure or system (repair or equipment, replacement of a part, re-installation of a network, etc.)."[354]

The other states also suggest that "damage" includes loss or disruption of functionality (Italy,[355] New Zealand[356]), impairment of operations of critical civilian infrastructure (Pakistan[357]), or neutralization (Japan[358]). Germany is more implicit, suggesting "harmful effects" on systems, information, objects or person, instead of speaking of "loss of functionality." Still, in light of the statement that "[t]he occurrence of physical damage, injury or death to persons or damage or destruction to objects comparable to effects of conventional weapons is not required for an attack in the sense of art. 49 para. 1" of API.[359] The German stance seems to resemble the other states above. Canada seems to subscribe to the same view as the German position, if what "harmful effect" means is the same as for Germany.[360]

(3) States that Have Not Taken a Position

Nine states raise the issue but do not discuss the "damage" requirement for "attack" in detail: Australia, Brazil, Denmark, Norway, Romania, Sweden, Switzerland, the UK and the U.S. While eleven other states do not refer to the issue at all, nine of them are contracting parties to API and ostensibly support the application of API Article 49 in cyber domain during an armed conflict: China, Czech Republic, Estonia, Finland, Iran, Kazakhstan, Kenya, the Netherlands, Poland and Russia.

3.7.4 Summary

TM2 Rule 92 (originally TM1 Rule 30) is built on Article 49(1) and other articles of Additional Protocol I. Concerning whether loss of functionality without physical damage can be recognized as an "attack," the majority of TM2 experts respond in the negative, while the minority and the ICRC disagree. State positions are also inconsistent, although numerous states have expressed their preference for the latter approach. At least from their standpoint, the Russian NotPetya attack on Ukraine appears to have produced the consequence necessary to amount to "attack," even though details on the harms suffered on the ground remain unknown. An unlawful "attack" in an armed conflict could be subject to criminal indictment as a war crime.

4 Potential Tasks for the Tallinn Manual 3.0 and Denmark

The previous chapter addressed seven topics that are controversial in both the Tallinn Manuals and among states. It examined how the discussion of those topics has evolved from TM1 to TM2 and whether the TM frameworks provide useful yardsticks for the legal assessment of actually occurring cyber incidents. Several observations and takeaways follow.

First, TM2 sometimes adopts different but less noticeable interpretations than TM1. Concerning the non-intervention rule, for example, the TM1 commentary referred to "the manipulation by cyber means of elections or of public opinion on the eve of elections"[361] as an example of prohibited intervention, while TM2 dropped "manipulation of public opinion" in its commentary, discussing intervention situations by "using cyber operations to remotely alter electronic ballots and thereby manipulate an election."[362] As for the state of necessity, the majority of TM2 experts excluded the interests of "international community as a whole" from protected interests under the rule on necessity,[363] unlike TM1, in which the experts unanimously supported its inclusion (although put in brackets).[364] Given that the international expert groups in TM1 and TM2 were generally different, it is understandable that their opinions sometimes varied. Nevertheless, the TMs are only four years apart, and there was seemingly no dramatic shift in state practice between their publication.

Second, as generative AI technology becomes more widespread, it seems likely that the legal grey zone concerning whether influence operations might amount to interference with "an inherently governmental function" for the rule of sovereignty and/or might amount to a prohibited intervention in the internal affairs of the target state will become more important. TM3 is expected to address these questions explicitly. The experts' conclusions will also significantly impact espionage-related questions. It is unlikely that the black-letter rule on espionage—that espionage *per se* is not prohibited under the *lex lata*—will change in TM3. But the notion of "an inherently governmental function" has yet to be clarified.[365] Depending on how widely the scope of such functions is expanded, more cases of espionage will be judged as illegal.

Third, it is important to note the risk of misapplying or abusing the plea of necessity. The TM2 commentary on necessity describes a prospective case in which a non-state actor in one state attacks another state. The victim state is entitled to invoke necessity on the ground that its essential interests are threatened by grave and imminent peril and no other state is responsible for the operation.[366] Here, the scenario for due diligence principle can be recalled. When Non-State Actor X located in State A, without having any connection to A, sets up a large botnet to launch a DDoS attack on State B, State A must exercise due diligence and take all feasible measures to thwart X's operation. As the due diligence principle is an obligation of conduct (not result),[367] State

A is not to blame for an unsuccessful outcome, unless it is unwilling[368] or fails to act rapidly enough despite reasonably having been able to do so.[369] Only in case of breach and the continuation of serious adverse consequences is State B entitled to take proportional countermeasures. Yet the countermeasures taken here are not to be directed against X, since "only States are subject to the international law prohibitions."[370] Thus, proportionality is assessed against the failure of due diligence by the territorial state.[371]

Suspicions arise as to whether State B might attempt to invoke the plea of necessity in this situation for reasons such as distrust of State A. The majority of TM2 experts argued that State B must solicit assistance from State A "if time permits and it is feasible to do so otherwise in the circumstances,"[372] which is not an absolute obligation; otherwise, State B may justify its necessity measures by emphasizing the urgency of the incidents. According to the minority view, State B does not even need to take urgency into account as a condition for the plea of necessity. It implies that necessity can be relied on regardless of State A's due diligence. Consequently, State A's sovereignty is violated against its will and State B is not held accountable for it. Some countries may fear such a scenario.

This risk of misapplication/abuse may not be on the TM3 agenda, because the plea of necessity is supposed to function independently of other doctrines. That said, it will be helpful for the interested states to urge the TM3 experts to clarify how necessity is employed; for example, by providing a concrete cyber scenario. According to the majority of TM2 experts, the test of "unwilling and unable" enables a state to breach a territorial state's sovereignty in the event of an armed attack. While the test remains controversial, it is easier to apply than the plea of necessity, because it sets a standard concerning the territorial state's behavior. It would be more helpful if similar conditions are set for the plea of necessity, such as what response by the territorial state will entitle/disentitle another state to invoke the plea.

Fourth, as to collective countermeasures, we can expect further elaboration from the TM3 experts. One task is to identify which obligations, if any, qualify for collective countermeasures when violated other than obligations *erga omnes*. Other conditions—such as the request by an injured state for assistance,[373] the gravity of the violation,[374] and the link to institutional sanctions—are also worth revisiting. As to the last point, in particular, the literature states that "the triggering of Chapter VII ends the power of States not individually injured to react as they please at the individual level."[375] The question then becomes whether and on what conditions that power applies to individual states if the Security Council fails to impose or increase sanctions. In that case, some states might want to resort to collective countermeasures by claiming that UN sanctions are no longer effective.

Fifth, as to extraterritorial enforcement jurisdiction, the TM3 experts will need to further investigate post-TM2 state practice. States that have engaged in relevant practice are encouraged to share their actions with the TM3 director and experts, NATO CCDCOE (which has the dedicated repository of data on state practice for the purpose of TM3), and other states. The Belgian case seems to contradict the TM2 view, as the Belgian court viewed the production order to a foreign service provider as a legitimate exercise of enforcement jurisdiction, and there might be similar cases. Such cases will require TM3 experts to rethink the issue of extraterritorial enforcement jurisdiction.

Sixth, and finally, as to the idea of "attack" in IHL, a certain number of states seem supportive of the minority/ICRC view. TM3 experts must pay more

attention to state perception and practice. Possible cyber war-crime cases in Ukraine deserve particular attention. In this regard, collaboration from all stakeholders and experts is essential to investigate these cases. As in the past TM editions, for which technical advisors joined an international group of experts, fully qualified technical experts must be made available to TM3. Similarly, with a view to conducting an impact analysis of attacks on healthcare entities in both peacetime and armed conflict, it is essential for TM3 experts to seek out assistance from medical and other relevant experts; moreover, military experts must clearly be enlisted to assess military cyber operations in Ukraine and other regions.

These potential tasks suggested for TM3 hold true for Denmark. Like all other states, Denmark is expected to be more transparent regarding its legal opinions and relevant national practice, particularly where it takes a minority position on an issue. The question of collective countermeasures is an excellent example, as Denmark sides with the TM2 experts on this point. Whether it advocates for the minority position as *lex lata* or *lex ferenda*, Denmark must engage more actively to convince other states and TM3 experts. Regardless of the issue, it is sensible for Denmark to articulate its own positions and engage with all the stakeholders involved in the TM3 project to ensure that its positions are represented in Tallinn Manual 3.0.

Notes

1 Michael Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge: Cambridge University Press, 2013, doi:10.1017/CBO9781139169288, https://www.cambridge.org/core/books/tallinn-manual-on-the-international-law-applicable-to-cyber-warfare/50C5BFF166A7FED75B4EA643AC677DAE

2 Michael Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2nd ed.), Cambridge: Cambridge University Press, 2017, doi:10.1017/9781316822524, https://www.cambridge.org/core/books/tallinn-manual-20-on-the-international-law-applicable-to-cyber-operations/E4FFD83EA790D7C4C3C28FC9CA2FB6C9

3 TM2, Introduction, https://www.cambridge.org/core/books/tallinn-manual-20-on-the-international-law-applicable-to-cyber-operations/introduction/D39A3D9EA7E5CD61022115B241193990, pp. 2–3.

4 This is a remark about TM1. Yet, the same holds true with TM2. Dieter Fleck, "Searching for International Rules Applicable to Cyber Warfare: A Critical First Assessment of the New Tallinn Manual," *Journal of Conflict and Security Law,* Volume 18, Issue 2, Summer 2013, pp. 331, 332, 351, https://doi-org.ep.fjernadgang.kb.dk/10.1093/jcsl/krt011

5 "The Tallinn Manual," NATO CCDCOE, https://ccdcoe.org/research/tallinn-manual/

6 NATO CCDCOE is one of twenty-eight international military organizations with NATO accreditation. For more details, "Centres of Excellence," NATO, December 6, 2022, https://www.nato.int/cps/en/natohq/topics_68372.htm

7 News "NATO Cooperative Cyber Defence Centre of Excellence grows to 25 members," NATO CCDCOE, June 13, 2019, https://ccdcoe.org/news/2019/nato-cooperative-cyber-defence-centre-of-excellence-grows-to-25-members/

8 Member States are expected to cooperate with the NATO CCDCOE to execute the research projects as necessary. In addition to making national experts available for the cyber exercises and a set of conferences at NATO CCDCOE, a questionnaire-based survey or interview is often conducted. See Damjan Štrucl, "Comparative study on the cyber defence of NATO Member States," NATO CCDCOE, 2021, https://ccdcoe.org/uploads/2022/04/Comparative-study-on-the-cyber-defence-of-NATO-Member-States.pdf; Taťána Jančárková and Grete Toompere, "National CERT/CSIRT: Mandate and Organisation," NATO CCDCOE, 2023, https://ccdcoe.org/uploads/2023/08/National_CERT-CSIRT_Mandate_and_Organisation_final_.pdf. Government experts of member states sometimes write a report on national regulation and practice. "Na-

tional Cybersecurity Organisation: ROMANIA," authored by Romanian government experts, NATO CCDCOE, 2020, https://ccdcoe.org/uploads/2020/11/NCS_organisation_ROM-2020_FINAL.pdf

9 Jeppe Mejer Kjelgaard and Ulf Melgaard, "Denmark's Position Paper on the Application of International Law in Cyberspace," *Nordic Journal of International Law*, July 4, 2023, https://brill.com/view/journals/nord/aop/article-10.1163-15718107-20230001/article-10.1163-15718107-20230001.xml

10 TM2, Introduction, p. 2.

11 Marc Schack and Astrid Kjeldgaard-Pedersen, "Modforanstaltninger i cyberdomænet: Den folkeretlige ramme" [Countermeasures in the cyber domain: The international legal framework], Djøf Publishing, August 2020, https://jura.ku.dk/pdf/icourts/research/Rapport_Modforanstaltninger_i_cyberspace.pdf (only in Danish); Idem, "Staters folkeretlige forpligtelse til at udvise 'due diligence' i cyberspace" [States' obligation under international law to exercise "due diligence" in cyberspace], Djøf Publishing, March 2022, https://static-curis.ku.dk/portal/files/305400398/Rapport_Staters_folkeretlige_forpligtelse_til_at_udvise_due_diligence_i_cyberspace_.pdf (only in Danish); Kevin Jon Heller, "Low-Intensity Cyber Operations and State Sovereignty in Cyberspace," Djøf Publishing, June 2022, https://cms.polsci.ku.dk/publikationer/low-intensity-cyber-operations-and-state-sovereignty-in-cyberspace/download-cms-rapport/CMS_Report_2022__5_-_Low-intensity_cyber_operations_and_state_sovereignty_in_cyberspace.pdf

12 Heller, "Low-Intensity Cyber Operations."

13 One survey confirms such documents released by 36 states in total. Duncan B. Hollis, "A Victim's Perspective on International Law in Cyberspace," *Lawfare*, August 28, 2023, https://www.lawfaremedia.org/article/a-victim-s-perspective-on-international-law-in-cyberspace

14 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, UN Doc. A/76/136, pp. 3–17, https://front.un-arm.org/wp-content/uploads/2021/08/A-76-136-EN.pdf

15 UN Doc. A/76/136, pp. 17–23

16 "International Law applicable in cyberspace," Government of Canada, April 22, 2022, https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/cyberspace_law-cyberespace_droit.aspx?lang=eng

17 "China's Positions on International Rules-making in Cyberspace," Ministry of Foreign Affairs, the People's Republic of China, October 20, 2021, https://www.fmprc.gov.cn/eng./wjb_663304/zzjg_663340/jks_665232/kjlc_665236/qtwt_665250/202110/t20211020_9594981.html; "China's Views on the Application of the Principle of Sovereignty in Cyberspace," Working

paper submitted by China to UN OEWG, December 2021, https://documents.unoda.org/wp-content/uploads/2021/12/Chinese-Position-Paper-on-the-Application-of-the-Principle-of-Sovereignty-ENG.pdf

18 "Costa Rica's Position on the Application of International Law in Cyberspace," Working paper submitted to UN Office for Disarmament Affairs, July 21, 2023, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Costa_Rica_-_Position_Paper_-_International_Law_in_Cyberspace.pdf

19 Statement by Special Envoy for Cyberspace at the 2nd substantive session of the UN OEWG, NÚKIB, February 11, 2020, https://www.nukib.cz/download/publications_en/CZ%20Statement%20-%20OEWG%20-%20International%20Law%2011.02.2020.pdf

20 "President Kaljulaid at CyCon 2019: Cyber attacks should not be easy weapon," *ERR News*, May 29, 2019, https://news.err.ee/946827/president-kaljulaid-at-cycon-2019-cyber-attacks-should-not-be-easy-weapon; UN Doc. A/76/136, pp. 23–30.

21 Marja Lehto, "Finland's Views on International Law and Cyberspace," *Nordic Journal of International Law*, 2023, https://brill.com/view/journals/nord/aop/article-10.1163-15718107-20230002/article-10.1163-15718107-20230002.xml (including an initially released paper in October 2020, Finnish MFA, "Finland Published Its Positions on Public International Law in Cyberspace," October 15, 2020, https://valtioneuvosto.fi/en/-/finland-published-its-positions-on-public-international-law-in-cyberspace). Hereinafter, the link to an English version at the bottom of the page is cited to as "Finland, position paper."

22 Le ministère des Armées, ed., *Droit international appliqué aux operations dans le cyberspace*, September 9, 2019, https://www.defense.gouv.fr/sites/default/files/ministere-armees/Droit%20international%20appliqu%C3%A9%20aux%20op%C3%A9rations%20dans%20le%20cyberespace.pdf; "International Law Applied to Operations in Cyberspace," paper shared by France with the open-ended working group established by Resolution 75/240, 2021, https://documents.unoda.org/wp-content/uploads/2021/12/French-position-on-international-law-applied-to-cyberspace.pdf

23 The Federal Government of Germany, "On the Application of International Law in Cyberspace," March 2021, https://www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf; UN Doc. A/76/136, pp. 31–44.

24 "General Staff of Iranian Armed Forces Warns of Tough Reaction to Any Cyber Threat," *Nournews*, August 18, 2020, https://nournews.ir/En/News/53144/General-Staff-of-Iranian-Armed-Forces-Warns-of-Tough-Reaction-to-Any-Cyber-Threat

25 "Ireland: Position Paper on the Application of International Law in Cyberspace," Working paper submitted to UN Office for Disarmament Affairs, July

7, 2023, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Ireland_-_National_Position_Paper.pdf

26 Roy Schöndorf, "Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations," *U.S. Naval War College International Law Studies*, Vol. 97, 2021, pp. 395–406, https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=2957&context=ils

27 "Italian Position Paper on 'International Law and Cyberspace'," Italian Ministry of Foreign Affairs and International Cooperation, November 2021, https://www.esteri.it/mae/resource/doc/2021/11/italian_position_paper_on_international_law_and_cyberspace.pdf

28 UN Doc. A/76/136, pp. 44–50.

29 UN Doc. A/76/136, pp. 51–52.

30 UN Doc. A/76/136, pp. 52–54.

31 UN Doc. A/76/136, pp. 54–65.

32 "The Application of International Law to State Activity in Cyberspace," Department of the Prime Minister and Cabinet of New Zealand, December 1, 2020, https://www.dpmc.govt.nz/publications/application-international-law-state-activity-cyberspace#:~:text=New%20Zealand%20is%20a%20champion,maintaining%20international%20peace%20and%20stability.

33 Vibeke Musæus, "Norway's Position Paper on International Law and Cyberspace," *Nordic Journal of International Law*, 2023, https://brill.com/view/journals/nord/aop/article-10.1163-15718107-20230003/article-10.1163-15718107-20230003.xml (including an initially released position in 2021, UN Doc. A/76/136, pp. 65–75). Hereinafter, the latter is cited as "Norway, position paper."

34 "Pakistan's Position on the Application of International law in Cyberspace," Working paper submitted to UN Office for Disarmament Affairs, March 3, 2023, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/UNODA.pdf

35 "The Republic of Poland's Position on the Application of International Law in Cyberspace," Ministry of Foreign Affairs of Republic of Poland, December 29, 2022, https://www.gov.pl/web/diplomacy/the-republic-of-polands-position-on-the-application-of-international-law-in-cyberspace

36 UN Doc. A/76/136, pp. 75–79.

37 UN Doc. A/76/136, pp. 79–82.

38 UN Doc. A/76/136, pp. 83–85.

39 Ola Engdahl, "Sweden's Position Paper on the Application of International Law in Cyberspace," *Nordic Journal of International Law*, 2023, https://brill.com/view/journals/nord/aop/article-10.1163-15718107-

20230004/article-10.1163-15718107-20230004.xml (including an initially released position paper in July 2022, Government Offices of Sweden, https://www.government.se/reports/2022/07/position-paper-on-the-application-of-international-law-in-cyberspace/)

40 UN Doc. A/76/136, pp. 85–105.

41 Speech "Cyber and International Law in the 21st Century," U.K. Government, May 23, 2018, https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century; UN Doc. A/76/136, pp. 106–136; Speech "International Law in Future Frontiers," May 19, 2022, https://www.gov.uk/government/speeches/international-law-in-future-frontiers

42 Remarks by Harold Hongju Koh, Legal Advisor U.S. Dept. of State, September 18, 2012, https://2009-2017.state.gov/s/l/releases/remarks/197924.htm; Submission by the U.S. to the 2014–15 UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security in October 2014, in CarrieLyn D. Guymon, Office of the Legal Adviser, U.S. Dept. of State, ed., *Digest of United States Practice in International Law*, 2014, pp. 732–740, https://2009-2017.state.gov/documents/organization/244504.pdf; Remarks on November 10, 2016 by Dept. of State Legal Advisor Brian J. Egan on international law and stability in cyberspace and submission by the U.S. to the 2016–2017 GGE, in idem., *Digest of United States Practice in International Law*, 2016, pp. 815–826, https://www.state.gov/wp-content/uploads/2019/05/2016-Digest-United-States.pdf; "DOD General Counsel Hon. Paul C. Ney, Jr. Remarks at U.S. Cyber Command Legal Conference," U.S. Dept. of Defense, March 2, 2020, https://www.defense.gov/News/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/

43 "Communiqué of the 1196th Meeting of the Peace and Security Council held on 29 January 2024 on the Common African Position on the Application of International Law to the Use of Information and Communication Technologies in Cyberspace," January 29, 2024, https://papsrepository.africa-union.org/bitstream/handle/123456789/2022/1196%20AU%20Common%20Position%20Adopted%20Version%20-%20EN.pdf?sequence=11

44 "Russia Begins Investigation into 2007 Bronze Night Murder in Tallinn," *ERR*, September 4, 2015, https://news.err.ee/116656/russia-begins-investigation-into-2007-bronze-night-murder-in-tallinn

45 "Under Siege: Events at the Estonian Embassy in Moscow," *ERR*, April 25, 2017, https://news.err.ee/592078/under-siege-events-at-the-estonian-embassy-in-moscow

46 Eneken Tikk, Kadri Kaska, and Liis Vihul, "International Cyber Incidents: Legal Considerations," NATO CCDCOE, 2010, pp. 23–24, https://ccdcoe.org/uploads/2018/10/legalconsiderations_0.pdf

47 Kadri Jakobson, "Eestist saab NATO kübersüda ja IT-polügoon" [Estonia to become NATO cyber-sanctuary and IT-pole] *Äripäiv*, May 18, 2007, https://www.aripaev.ee/uudised/2007/05/17/eestist-saab-nato-kubersuda-ja-it-polugoon?hasAccess=false; "The Kremlin would be able to inflict a lot more

cyber damage if it chose to do so, such as an attack on national power grids, energy and industrial processes;" James Pamment, Vladimir Sazonov, Francesca Granelli, Sean Aday, Māris Andžāns, Una Bērziņa-Čerenkova, John-Paul Gravelines, Mils Hills, Miranda Holmstrom, Adam Klus, Irene Martinez-Sanchez, Mariita Mattiisen, Holger Molder, Yeganeh Morakabati, Aurel Sari, Gregory Simons, and Jonathan Terra, "Hybrid Threats: 2007 Cyber Attacks on Estonia," NATO Strategic Communications Centre of Excellence, 2019, p. 67, https://stratcomcoe.org/publications/hybrid-threats-2007-cyber-attacks-on-estonia/86, p. 62.

48 Any activity that makes a service unavailable for use by legitimate users or delays system operations and functions. "Glossary," Canadian Centre for Cyber Security, https://www.cyber.gc.ca/en/glossary#d

49 An attack in which multiple compromised systems are used to attack a single target. The flood of incoming messages to the target system forces it to shut down and denies service to legitimate users. Ibid.

50 Rain Ottis, "Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective," NATO CCDCOE, https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf; Jakobson, "Eestist saab NATO kübersüda."

51 Thomas Rid, *Cyber War Will Not Take Place*, Oxford University Press, 2013, p. 6.

52 Jakobson, "Eestist saab NATO kübersüda."

53 Pamment et al., "Hybrid Threats: 2007 Cyber Attacks."

54 Ottis, "Analysis of the 2007 Cyber Attacks," p. 4.

55 Pamment et al., "Hybrid Threats: 2007 Cyber Attacks," p. 56.

56 "During the 2007 cyber attack on Estonia, several Estonian officials raised the issue of whether Article 5 of the North Atlantic Treaty Organization (NATO) could be invoked." Scott J. Shackelford, "State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem," in Christian Czosseck and Karlis Podins, eds., *Conference on Cyber Conflict*: Proceedings 2010, 2010, p. 204, https://ccdcoe.org/uploads/2018/10/1_Proceedings2010FullBook.pdf

57 Rex B. Hughes, "NATO and Cyber Defence: Mission Accomplished?" *Atlantisch Perspectief*, 2009nr1/4, p. 1, https://csl.armywarcollege.edu/SLET/mccd/CyberSpacePubs/NATO%20and%20Cyber%20Defence%20-%20Mission%20Accomplished.pdf

58 NATO, "NATO Opens New Centre of Excellence on Cyber Defence," NATO, May 14, 2008, https://www.nato.int/docu/update/2008/05-may/e0514a.html

59 Bucharest Summit Declaration Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Bucharest on 3 April 2008, NATO, April 3, 2008, https://www.nato.int/cps/en/natolive/official_texts_8443.htm

60 NATO, "Cyber Defence," September 14, 2023, https://www.nato.int/cps/en/natohq/topics_78170.htm

61 Rid, *Cyber War*, p. 7.

62 Jakobson, "Eestist saab NATO kübersüda;" Pamment et al., "Hybrid Threats: 2007 Cyber Attacks," p. 67; "NATO CCDCOE: Expertise and Cooperation Make Our Cyber Space Safer," e-Estonia, October 16, 2018, https://e-estonia.com/nato-ccdcoe-expertise-cyber-space-safer/

63 NATO, "NATO Opens New Centre."

64 "Centre Is the First International Military Organization Hosted by Estonia," NATO CCDCOE, October 28, 2008, https://ccdcoe.org/news/2008/centre-is-the-first-international-military-organization-hosted-by-estonia/

65 See "Centres of Excellence," especially about a section on "How Does NATO request Centres of Excellence Products and Services?", NATO Allied Command Transformation (ACT), https://www.act.nato.int/about/centres-of-excellence/

66 Michael N. Schmitt, "Computer Network and the Use of Force in International Law: Thought on a Normative Framework," *Columbia Journal of Transnational Law*, Volume 37, 1999, p. 885.

67 Video "CyCon 2012 | Michael Schmitt: Tallinn Manual Part I," U.S. Naval War College, September 29, 2012, https://www.youtube.com/watch?v=wY3uEoltso

68 The exact selection process is unknown, but it is assumed that (except for technical experts, a project manager, and coordinator, which are mainly managed by the NATO CCDCOE) the TM director decided on an overall membership of international law experts.

69 Michael N. Schmitt, Charles H.B. Garraway, and Yoram Dinstein, *The Manual on the Law of Non-International Armed Conflict*, International Institute of Humanitarian Law, 2006.

70 Program on Humanitarian Policy and Conflict Research (HPCR) at Harvard University, ed., *HPCR Manual on International Law Applicable to Air and Missile Warfare*, Cambridge: Cambridge University Press, 2013, doi:10.1017/CBO9781139525275, https://www.cambridge.org/core/books/hpcr-manual-on-international-law-applicable-to-air-and-missile-warfare/EB28F7A1701637CA2390B25FB4840629

71 The U.S. Naval Postgraduate School, Faculty Profile Directory on James B Michael, https://nps.edu/faculty-profiles/-/cv/bmichael

72 TM2, p. 1.

73 "About the NATO CCDCOE," in Karlis Podins, Jan Stinissen, Markus Maybaum, ed., *Proceedings of 5th International Conference on Cyber Conflict (CyCon)*, June 2013, https://ccdcoe.org/uploads/2018/10/CyCon_2013_Proceedings.pdf

74 TM2, Introduction, p. 6.

75 Fleck, "Searching for International Rules," pp. 332–335.

76 TM2, Introduction.

77 Remarks by Schmitt in the session entitled "CyCon 2022, Day 2 Panel: Tallinn Manual 3.0 Achievements, Shortcomings, Prospects," held on June 2, 2022, https://www.youtube.com/watch?v=2papcgw2888&t=81s

78 NATO CCDCOE, news release, "Over 50 States Consult Tallinn Manual 2.0," February 2, 2016, https://ccdcoe.org/news/2016/over-50-states-consult-tallinn-manual-2-0/

79 TM1 Introduction, pp. 5, 11; TM2 Introduction, pp. 2, 3, 5.

80 Ibid., p. 14.

81 Ibid., p. 574.

82 TM1, Introduction, p. 5; TM2 Introduction, pp. 3–4. *Lex lata* means "Ratified law." The positive law currently in force, without modification to account for any rules subjectively preferred by the interpreter. *Oxford Reference*, https://www.oxfordreference.com/display/10.1093/acref/9780195369380.001.0001/acref-9780195369380-e-1247

83 *Lex ferenda* translates to "Law to be proposed"; that is, the law considered to be normatively preferable when the existing rule of law causes an unclear or undesirable result. Lex ferenda is, thus, a proposed law or proposed interpretation of a law rather than a statement of law in force as reflected by positive sources of authority. *Oxford Reference*, https://www.oxfordreference.com/display/10.1093/acref/9780195369380.001.0001/acref-9780195369380-e-1239

84 TM1 Introduction, p. 5.

85 Both TMs recognize the possible application of a persistent objector. TM1 Introduction, p. 6; TM2 Introduction, p. 4.

86 TM1 Introduction, p. 6; TM2 Introduction, p. 4.

87 Schmitt, "Tallinn Manual 2.0 on the International Law of Cyber Operations: What It Is and Isn't," *Just Security*, February 9, 2017, https://www.justsecurity.org/37559/tallinn-manual-2-0-international-law-cyber-operations/

88 Idem, "'Virtual' Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law," *Chicago Journal of International Law*, Vol. 19, 2018, pp. 46, 50, 66, https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=1736&context=cjil

89 Schmitt, "Tallinn Manual 2.0: What It Is and Isn't."

90 International Cyber Law in Practice: Interactive Toolkit, NATO CCDCOE, https://cyberlaw.ccdcoe.org/wiki/Main_Page; Kubo Mačák, Tatiana Jančárková, and Tomáš Minárik, "The Right Tool for the Job: How Does Inter-

national Law Apply to Cyber Operations?," *the ICRC Humanitarian Law & Policy Blog*, October 6, 2020, https://blogs.icrc.org/law-and-policy/2020/10/06/international-law-cyber-operations/

91 Statute of the International Court of Justice, https://www.icj-cij.org/statute

92 Christopher Greenwood, "Outline of Sources of International Law: An Introduction," *UN Audio Library of International Law*, pp. 1–2, https://legal.un.org/avl/pdf/ls/greenwood_outline.pdf

93 Ibid., p. 3.

94 Ibid.

95 Ibid., p. 4.

96 Michael N. Schmitt and Liis Vihul, "The Nature of International Law Cyber Norms," *Tallinn Papers*, No. 5, NATO CCDCOE, 2014, p. 31, https://ccdcoe.org/uploads/2018/10/Tallinn-Paper-No-5-Schmitt-and-Vihul.pdf; Idem, "Respect for Sovereignty in Cyberspace," *Texas Law Review*, Vol. 95, 2017, p. 1650, https://texaslawreview.org/wp-content/uploads/2017/11/Schmitt.Vihul_.pdf

97 NATO CCDCOE, "Contribute to the Tallinn Manual 3.0," https://customervoice.microsoft.com/Pages/ResponsePage.aspx?id=Soev6_HZQE6E0qvVZ2coeDgkvv4LP1FBg_gf1jtxncZUMDdXVEcwSUdZUzU3RVRXQkhFTFZNMlpBUi4u

98 Schmitt, "CyCon 2022, DAY 2 Panel."

99 TM1, Introduction, p. 5; TM2 Introduction, p. 3.

100 William Boothby, "Cyber Deception and Autonomous Attack: Is There a Legal Problem?" in Podins, Stinissen, and Maybaum, *Proceedings of 5th CyCon*, p. 246.

101 The ICRC, International Humanitarian Law Database, https://ihl-databases.icrc.org/en/ihl-treaties/hague-conv-iv-1907?activeTab=default. There are older documents in this regard, such as the Lieber Code and the Brussels Declaration. For more details about the history, see the ICRC, Customary IHL Database, https://ihl-databases.icrc.org/en/customary-ihl/v1/rule107#title-3

102 Schmitt, "CyCon 2022, DAY 2 Panel."

103 The ICRC, *Commentary of Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977*, 1987, para. 1775, https://ihl-databases.icrc.org/en/ihl-treaties/api-1977/article-46/commentary/1987?activeTab=1949GCs-APs-and-commentaries

104 Ibid., https://ihl-databases.icrc.org/en/ihl-treaties/api-1977?activeTab=default

105 Emphasis added by author.

106 TM1 Rule 66 commentary, p. 193, para. 2.

107 Ibid., para. 3.

108 TM1 Rule 66 commentary, p. 194, para. 5.

109 TM1 Rule 66 commentary, p. 193, para. 2, n. 254.

110 Emphasis added by author. The ICRC, Customary IHL database, 2005, Rule 107 [Spies], https://ihl-databases.icrc.org/en/customary-ihl/v1/rule107#Fn_BE18BC66_00004

111 Emphasis added by author.

112 TM2 Rule 89 commentary, p. 411, para. 7, n. 995. *In U.S. DoD's Law of Manual* (2015. Update in December 2016), p. 149, para. 4.17.2 on Spies stipulates as follows (Emphasis added by author).

> A person may only be considered a spy when, (1) acting clandestinely or under false pretenses, (2) in the zone of operations of a belligerent, (3) he or she obtains, or endeavors to obtain, information, (4) with the intention of communicating it to the hostile party. During war, any person—military or civilian—whose actions meet all of these elements may be considered a spy under the law of war.

https://dod.defense.gov/Portals/1/Documents/pubs/DoD%20Law%20of%20War%20Manual%20-%20June%202015%20Updated%20Dec%202016.pdf?ver=2016-12-13-172036-190. The same document last updated in July 2023 by the U.S. DoD maintains the same sentences for the paragraph on the subject, pp. 150–151, para. 4.17.2, https://media.defense.gov/2023/Jul/31/2003271432/-1/-1/0/DOD-LAW-OF-WAR-MANUAL-JUNE-2015-UPDATED-JULY%202023.PDF

113 E.g., the critic listed the technical problems in determining the actual location of a cyber spy and the capabilities of VPN technology. Sergei Yulievish Garkusha-Bozhko, "The Problem of Cyber Espionage in the International Humanitarian Law" [ПРОБЛЕМА КИБЕРШПИОНАЖА В МЕЖДУНАРОДНОМ ГУМАНИТАРНОМ ПРАВЕ], *Moscow Journal of International Law*, No. 1, 2021, pp. 70–80, https://www.mjil.ru/jour/article/view/396/288

114 Samantha Besson, "Sovereignty," *Max Planck Encyclopedia of Public International Law*, April 2011, https://opil-ouplaw-com.ep.fjernadgang.kb.dk/display/10.1093/law:epil/9780199231690/law-9780199231690-e1472?rskey=gfkpmf&result=1&prd=MPIL

115 TM2, p. 17.

116 TM2 Rule 4 commentary, pp. 20–21, para. 13.

117 TM2 Rule 4 commentary, pp. 21–22, paras. 15–17.

118 TM2 Rule 32 commentary, p. 170, para. 6.

119 TM2, Rule 4 commentary, p. 19, para. 8.

120 TM1 Rule 6 commentary, p. 30, para. 4.

121 TM2, p. 168.

122 TM2 Rule 32 commentary, p. 169, para. 5.

123 TM2 Rule 32 commentary, p. 170, para. 6.

124 TM2 Rule 32 commentary, p. 173, para. 14.

125 TM2 Rule 4 commentary, p. 22, para. 16.

126 TM2 Rule 32 commentary, pp. 170–171, para. 8.

127 TM2 Rule 32 commentary, pp. 170–171, para. 9.

128 TM2 Rule 32 commentary, pp. 171–172, para. 10.

129 TM2 Rule 32 commentary, p. 172, para. 11.

130 See Michaela Prucková, ed., "SolarWinds (2020)," in NATO CCDCOE, International Cyber Law in Practice: Interactive Toolkit, June 3, 2021, https://cyberlaw.ccdcoe.org/wiki/SolarWinds_(2020)

131 NATO CCDCOE, "Recent Cyber Events and Possible Implications for Armed Forces, No. 8: A Look at the Trends from 2020 and towards the Future," January 2021, p. 1, https://ccdcoe.org/uploads/2021/01/Recent-Cyber-Events-and-Possible-Implications-for-Armed-Forces-8-January-2021_Final-1.pdf

132 Tomáš Minárik, ed., "NotPetya (2017)," in NATO CCDCOE, International Cyber Law in Practice: Interactive Toolkit, November 14, 2022, https://cyberlaw.ccdcoe.org/wiki/NotPetya_(2017); Craig Timberg, Ellen Nakashima, Hannes Munzinger; Hakan Tanriverdi, "Secret Trove Offers Rare Look into Russian Cyberwar Ambitions," *The Washington Post*, March 30, 2023.

133 Joe Weiss and Bob Hunter, "The SolarWinds Hack Can Directly Affect Control Systems," *Lawfare*, January 22, 2021, https://www.lawfaremedia.org/article/solarwinds-hack-can-directly-affect-control-systems

134 TM2 Rule 32 commentary, pp. 172–173, para. 13.

135 National Institute of Standards and Technology (NIST) of U.S., Glossary, https://csrc.nist.gov/glossary/term/honeypot

136 TM2 Rule 32 commentary, p. 174, para. 16.

137 Office of the Director of National Intelligence (ODNI), "Assessing Russian Activities and Intentions in Recent US Elections," JCA 2017-01D, January 6, 2017, https://www.dni.gov/files/documents/ICA_2017_01.pdf

138 Schmitt, "'Virtual' Disenfranchisement," p. 36, especially, n. 32.

139 Ibid., p. 47.

140 Ibid., p. 45.

141 TM2 Rule 32 commentary, pp. 171–172, para. 10.

142 Ibid., p. 172, para. 11.

143 Schmitt, "'Virtual' Disenfranchisement," p. 46.

144 The U.S. Department of Justice, press release, "Grand Jury Indicts 12 Russian Intelligence Officers for Hacking Offenses Related to the 2016 Election," July

13, 2018, https://www.justice.gov/opa/pr/grand-jury-indicts-12-russian-intelligence-officers-hacking-offenses-related-2016-election

145 Taťána Jančárková, Kubo Mačák, and Tomáš Minárik, "Scenario 01: Election Interference," in NATO CCDCOE, International Cyber Law in Practice: Interactive Toolkit, February 2, 2023, https://cyberlaw.ccdcoe.org/wiki/Scenario_01:_Election_interference. Of the four Nordic countries, Denmark, Finland, and Norway, but not Sweden refer to this point. Presumably, they support the conclusion in the text. Kjelgaard and Melgaard, "Denmark's Position Paper," p. 449; Finland, position paper, p. 2; Norway, position paper, UN Doc. A/76/136, p. 68.

146 *North Sea Continental Shelf, Judgment, I.C.J. Reports 1969*, p. 43, para. 74, https://www.icj-cij.org/public/files/case-related/52/052-19690220-JUD-01-00-EN.pdf

147 "Importantly, some cyber activities, such as cyber espionage, do not amount to a breach of territorial sovereignty, and hence to a violation of international law." Canada, position paper, para. 19.

148 "…once a piece of malware successfully enters a system or network, it remains a latent threat to its integrity. This may damage software or hardware and thus interfere with the conduct of State affairs. Furthermore, surveillance operations may be carried out in ways that lead to breaches of State sovereignty or other rules of international law. As such, Costa Rica believes that, in some circumstances, cyber espionage may amount to a breach of State sovereignty." Costa Rica, position paper, pp. 6–7, para. 22.

149 "L'espionnage informatique, qui n'est pas illicite en droit international bien qu'il puisse méconnaitre ce droit lorsqu'il est associé à un fait internationalement illicite, ne fait pas l'objet d'une analyse ou de développements spécifiques dans le présent document." Le ministère des Armées, *Droit international appliqué aux operations dans le cyberspace*, p. 4, para. 2.

150 "There is a range of circumstances – in addition to pure espionage activity – in which an unauthorised cyber intrusion, including one causing effects on the territory of another state, would not be internationally wrongful." New Zealand, position paper, p. 3, para. 14.

151 "…cyber espionage … not in itself illegal under international law." UN Doc. A/76/136, 2021, p. 66, no. 176.

152 "There is no per se prohibition on such activities under customary international law. I would caution, however, that because 'intelligence collection' is not a defined term, the absence of a per se prohibition on these activities does not settle the question of whether a specific intelligence collection activity might nonetheless violate a provision of international law." Remarks by Egan, in *Digest of U.S. Practice in International Law*, 2016, p. 818; "Of course, most countries, including the United States, have domestic laws against espionage, but international law, in our view, does not prohibit espionage per se even when it involves some degree of physical or virtual intrusion into foreign ter-

ritory. There is no anti-espionage treaty, and there are many concrete examples of States practicing it, indicating the absence of a customary international law norm against it." Remarks by Ney, Jr.

153 "China's Views on the Application of the Principle of Sovereignty in Cyberspace," p. 2.

154 "Any utilization of cyberspace if and when involves unlawful intrusion to the (public or private) cyber structures which is under the control of another state, may be constituted as the violation of the sovereignty of the targeted state." Iran, position paper, para. 4.

155 UN Doc. A/76/136, p. 87. Switzerland is categorized as the pure-sovereigntist position. Heller, "Low-Intensity Cyber Operations," pp. 26–27.

156 "The [AU] affirms that by virtue of territorial sovereignty, any unauthorized access by a State into the ICT infrastructure located on the territory of a foreign State is unlawful. Therefore, the African Union emphasizes that the obligation to respect the territorial sovereignty of States, as it applies in cyberspace, does not include a de minimis threshold of harmful effects below which an unauthorized access by a State into the ICT infrastructure located on the territory of a foreign State would not be unlawful." See the AU position paper, para. 16.

157 TM2 Rule 32 commentary, pp. 170–171, n. 387.

158 *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Merits, Judgment, I.C.J. Reports 1986*, p. 106, para. 202, https://www.icj-cij.org/sites/default/files/case-related/70/070-19860627-JUD-01-00-EN.pdf

159 UN Doc. A/76/135, IV, para. 71 (c).

160 TM1 Rule 10 commentary, p. 44, para. 7.

161 TM1 Rule 10 commentary, p. 45, para. 9.

162 Ibid, para. 10.

163 TM2, p. 312.

164 TM2 Rule 66 commentary, p. 314, para. 6.

165 TM2 Rule 66 commentary, p. 315, para. 8.

166 Schmitt, "'Virtual' Disenfranchisement," p. 49.

167 Emphasis added by author. Marko Milanović and Michael Schmitt, "Cyber Attacks and Cyber (Mis)information Operations during a Pandemic," *Journal of National Security Law & Policy*, Vol. 11, 2020, pp. 247, 255, https://jnslp.com/wp-content/uploads/2020/12/Cyber-Attacks-and-Cyber-Misinformation-Operations-During-a-Pandemic_2.pdf; The Cyber Law Toolkit series run by NATO CCDCOE supports this view but does not necessarily limit the scope to the pandemic. "Scenario 20: Cyber operations against medical

facilities," in NATO CCDCOE Cyber Law Toolkit, https://cyberlaw.ccdcoe.org/wiki/Scenario_20:_Cyber_operations_against_medical_facilities#cite_ref-37

168 TM2 Rule 66 commentary, p. 315, para. 9.

169 TM2 Rule 66 commentary, pp. 317–318, para. 18.

170 TM2 Rule 66 commentary, p. 318, para. 20.

171 TM2 Rule 66 commentary, pp. 322–323, para. 30.

172 TM2 Rule 66 commentary p. 318, para. 19.

173 TM2 Rule 66 commentary p. 320, para. 24.

174 TM2 Rule 66 commentary pp. 320–321, para. 25.

175 Milanović and Schmitt, "Cyber Attacks and Cyber (Mis)information," pp. 269–270.

176 Schmitt, "'Virtual' Disenfranchisement," pp. 50–51.

177 Ibid., p. 51.

178 WannaCry is a piece of malware that encrypts important data on infected systems to extort money from the victim. Federal Cyber Security Authority of Germany (BSI), https://www.bsi.bund.de/EN/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Botnetze/Steckbriefe-aktueller-Botnetze/Steckbriefe/Wannacry/Wannacry.html; Mihkel Pikkat, ed., "WannaCry (2017)," in NATO CCDCOE, International Cyber Law in Practice: Interactive Toolkit, June 3, 2021, https://cyberlaw.ccdcoe.org/wiki/WannaCry_(2017)

179 Milanović and Schmitt, "Cyber Attacks and Cyber (Mis)information," p. 256. Emphasis in original.

180 Ibid., p. 258. Emphasis added by author.

181 Ibid.

182 "…the notion of injury extends from cyber operations resulting in death to those merely affecting health in some manner. Thus, by the prevailing view, any of the cyber operations attributable to a state that have negatively affected the health of any individuals on the state's territory, as did those that interfered with the immediate delivery of medical care, violated the sovereignty of that state." Ibid., p. 253. Emphasis added by author. Apart from legal issues, it is a challenging task to quantify harm caused to patients. "Despite the number of reported cyberattacks on healthcare internationally, there is paucity of information on the actual impact of any attack in terms of service disruption, financial impact, and harm to patients." Saira Ghafur, Søren Rud Kristensen, Kate Honeyford, et al. "A Retrospective Impact Analysis of the WannaCry Cyberattack on the NHS. *npj Digital Medicine*, Vol. 2, 2019, https://doi.org/10.1038/s41746-019-0161-6

183 Ransomware is a type of malware that denies a user's access to a system or data until a sum of money is paid. Canadian Centre for Cyber Security, https://www.cyber.gc.ca/en/guidance/ransomware#defn-ransomware

184 UN Doc. A/76/136, p. 5.

185 Costa Rica, position paper, pp. 7–8.

186 Denmark, position paper, p. 5.

187 Estonia, position paper, UN Doc. A/76/136, p. 25.

188 Finland, position paper, pp. 8–9.

189 Germany, position paper, UN Doc. A/76/136, pp. 34–35.

190 Norway, position paper, UN Doc. A/76/136, pp. 9–10.

191 Poland, position paper, p. 4.

192 Switzerland, position paper, UN Doc. A/76/136, pp. 87–88.

193 Norway, position paper, UN Doc. A/76/136, p. 69. Emphasis added by author.

194 New Zealand, position paper, p. 2, para. 9 (b).

195 U.K. government, "International Law in Future Frontiers," May 19, 2022.

196 "Its content varies between different primary rule-sets in international law." Timo Koivurova and Krittika Singh, "Due Diligence," *Max Planck Encyclopedia of Public International Law*, August 2022, Sec. A, paras. 2–3, https://opil-ouplaw-com.ep.fjernadgang.kb.dk/display/10.1093/law:epil/9780199231690/law-9780199231690-e1034?rskey=ZHYzzQ&result=1&prd=MPIL

197 More specifically, in the context of the case, the question was not "whether Albania had exercised due diligence," as the Court pronounced that "the laying of the minefield which caused the explosions on October 22, 1946, could not have been accomplished without the knowledge of the Albanian Government. The obligations resulting for Albania from this knowledge are not disputed between the Parties." *Corfu Channel case, Judgment of April 9th, 1949: I.C. J. Reports 1949*, p. 22, https://www.icj-cij.org/sites/default/files/case-related/1/001-19490409-JUD-01-00-EN.pdf; Michael Waibel, "Corfu Channel Case," *Max Planck Encyclopedia of Public International Law*, March 2013, para. 9, https://opil-ouplaw-com.ep.fjernadgang.kb.dk/display/10.1093/law:epil/9780199231690/law-9780199231690-e118

198 TM2 Rule 2 commentary, p. 16, para. 12.

199 TM1 Rule 5 commentary, p. 28, para. 11.

200 TM1, p. 26.

201 TM1 Rule 5 commentary, p. 28, para. 11.

202 TM1 Rule 5 commentary, pp. 28–29, para. 12.

203 TM1 Rule 5 commentary, p. 29, para. 13.

204 TM1 Rule 13 commentary, p. 61, paras. 23–24.

205 UN Doc. A/68/98, para. 23.

206 UN Doc. A/70/174, para. 13 (c).

207 TM2 Rule 6 commentary, pp. 33–34, paras. 13–14.

208 TM2 Rule 6 commentary, p. 41, paras. 39–40.

209 TM2 Rule 6 commentary, p. 33, para. 13.

210 TM2 Rule 6 commentary, p. 34, para. 14.

211 TM2 Rule 6 commentary, pp. 38–39, para. 31.

212 TM2 Rule 6 commentary, p. 41, para. 39, Esp. n. 52

213 "A vulnerability in OpenSSL could allow a remote attacker to expose sensitive data, possibly including user authentication credentials and secret keys, through incorrect memory handling in the TLS heartbeat extension." U.S. Cybersecurity &Infrastructure Security Agency (CISA), "OpenSSL 'Heartbleed' vulnerability (CVE-2014-0160)," October 5, 2016, https://www.cisa.gov/news-events/alerts/2014/04/08/openssl-heartbleed-vulnerability-cve-2014-0160; The attack is said to have originated in China. Jim Finkle and Supriya Kurane, "U.S. hospital breach biggest yet to exploit Heartbleed bug: expert," *Reuters*, August 20, 2014, https://www.reuters.com/article/us-community-health-cybersecurity-idUSKBN0GK0H420140820

214 TM2 Rule 6 commentary, p. 41, para. 40.

215 TM2, p. 30.

216 TM2 Rule 6 commentary, p. 34, para. 15.

217 TM2 Rule 6 commentary, p. 35, para. 21.

218 TM2 Rule 6 commentary, pp. 36–37, para. 25.

219 TM2 Rule 6 commentary, p. 37, para. 26.

220 TM2 Rule 6 commentary, p. 37, para. 27.

221 TM2 Rule 6 commentary, pp. 37–38, para. 28.

222 TM2, p. 43.

223 TM2 Rule 7 commentary, p. 49, para. 24.

224 TM2 Rule 23 commentary, p. 130, para. 11.

225 TM2, p. 116.

226 *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Merits, Judgment, I.C.J. Reports 1986*, p. 14.

227 TM1 Rule 11 commentary, pp. 46–47, paras. 4–5; TM2 Rule 69 commentary, pp. 331–332, paras. 4–5.

228 TM1 Rule 13 commentary, pp. 60–61, para. 23; TM2 Rule 71 commentary, p. 347, para. 25.

229 TM1 Rule 13 commentary, pp. 60–61, para. 23; TM2 Rule 71 commentary, pp. 347–348, para. 25.

230 Paul Szoldra, "Inside the Hacker Underworld of ISIS," *Insider*, June 16, 2016, https://www.businessinsider.com/isis-hacking-division-operates-2016-6?r=US&IR=T

231 "China's Views on the Application of the Principle of Sovereignty in Cyberspace," pp. 2–3.

232 UN Doc. A/76/136, 2021, p. 141.

233 Ibid., para. 13.

234 UN Doc. A/76/136, p. 84, para. 14.

235 The U.S. paper submitted to UN cyber GGE, in Digest of US Practice in International Law, 2014, p. 735.

236 Tess Bridgeman, "When Does the Legal Basis for U.S. Forces in Syria Expire? The End Point of the 'Unwilling or Unable' Theory of Self-Defense," *Just Security*, March 14, 2018, https://www.justsecurity.org/53810/legal-basis-u-s-forces-syria-expire/; Chris Ray, "War Laws Are 'Challenged' in Syria, East Asia," *The Australian*, March 2, 2018.

237 Elena Chachko and Ashley Deeks, "Which States Support the 'Unwilling and Unable' Test?," *Lawfare*, October 16, 2016, https://www.lawfaremedia.org/article/which-states-support-unwilling-and-unable-test. Denmark is grouped in "ambiguous cases" along with Colombia, Ethiopia, France, the members of the the Gulf Cooperation Council (GCC; Egypt, Iraq, Jordan and Lebanon), India, Norway, Portugal, Rwanda and Uganda. As regards Denmark and Norway, however, their supportive positions were more clearly shown in the statements and documents in their native languages at that time. Marc Schack, "Resisting Clarity: Scandinavian Ambiguity in the 'Unable or Unwilling'-Debate," *Nordic Journal of International Law*, Vo. 90, 2021, pp. 31–59, https://brill-com.ep.fjernadgang.kb.dk/view/journals/nord/90/1/article-p31_31.xml

238 Le ministère des Armées, *Droit international appliqué aux operations dans le cyberspace*, p. 10; France, position paper, p. 8.

239 Chachko and Deeks, "Which States Support the 'Unwilling and Unable' Test?"

240 James Crawford, *The International Law Commission's Articles on State Responsibility: Introduction, Text and Commentaries*, Cambridge University Press, 2002, p. 160.

241 It provides that "This Chapter [countermeasures] does not prejudice the right of any State … to invoke the responsibility of another State, to take lawful measures against that State to ensure cessation of the breach and reparation in the interest of the injured State or of the beneficiaries of the obligation

breached." "Lawful measures" can be interpreted as meaning countermeasures, as their unlawfulness is precluded when taken in conformity with various conditions in article 49 to 53. Linos-Alexandre Sicilianos, "Countermeasures in Response to Grave Violations of Obligations Owed to the International Community," in James Crawford, Alain Pellet, Simon Olleson, and Kate Parlett, eds., *The Law of International Responsibility*, Oxford University Press, 2010, p. 1145.

242 Crawford, *ILC's Articles on State Responsibility*, pp. 169, 283.

243 Ibid., p. 305, commentary, para. 6.

244 Remarks by Prof. Martti Koskenniemi speaking on behalf of Nordic countries, at the Sixth Committee of the UN General Assembly, UN Doc. A/C.6/56/SR.11, p. 6, para. 33, https://undocs.org/Home/Mobile?FinalSymbol=A%2FC.6%2F56%2FSR.11&Language=E&DeviceType=Desktop&LangRequested=False

245 Sicilianos, "Countermeasures in Response to Grave Violations," p. 1142; Pierre-Marie Dupuy, "The Deficiencies of the Law of State Responsibility Relating to Breaches of 'Obligations Owed to the International Community as a Whole': Suggestions for Avoiding the Obsolescence of Aggravated Responsibility," in The Late Antonio Cassese, ed., *Realizing Utopia: The Future of International Law*, Oxford University Press, 2012, p. 216.

246 TM1 Rule 9 commentary, pp, 36–41.

247 TM2 Rule 24 commentary, p. 131, para. 5.

248 TM2, p. 130.

249 TM2 Rule 24 commentary, p. 132, para. 7.

250 Crawford, *ILC's Articles on State Responsibility*, Article 54 commentary, pp. 302–304, para. 3.

251 Ibid, p. 304, para. 4.

252 TM2 Rule 24 commentary, p. 132, paras. 8–9.

253 Marco Roscini, "Cyber Operations as Nuclear Counterproliferation Measures," *Journal of Conflict and Security Law*, Vol. 19, Issue 1, 2014, pp. 142, 145–146.

254 "Trump approved cyber-strikes against Iranian computer database used to plan attacks on oil tankers," *The Washington Post*, June 22, 2019, https://www.washingtonpost.com/world/national-security/with-trumps-approval-pentagon-launched-cyber-strikes-against-iran/2019/06/22/250d3740-950d-11e9-b570-6416efdc0803_story.html?noredirect=on; "Exclusive: U.S. carried out secret cyber strike on Iran in wake of Saudi oil attack: officials," *Reuters*, October 16, 2019, https://www.reuters.com/article/us-usa-iran-military-cyber-exclusive-idUSKBN1WV0EK

255 Robert Chesney, "The Legal Context for CYBERCOM's Reported Operations against Iran," *Lawfare*, June 24, 2019, https://www.lawfaremedia.org/article/legal-context-cybercoms-reported-operations-against-iran; Idem, "A

Cyber Command Operational Update: Clarifying the June 2019 Iran Operation," *Lawfare*, September 3, 2019, https://www.lawfaremedia.org/article/cyber-command-operational-update-clarifying-june-2019-iran-operation

256 Michael Schmitt, "Three International Law Rules for Responding Effectively to Hostile Cyber Operations," *Just Security*, July 13, 2021, https://www.justsecurity.org/77402/three-international-law-rules-for-responding-effectively-to-hostile-cyber-operations/

257 Ibid.

258 As for an operation in 2020 to take down a TricBot botnet, see Ellen Nakashima, "Cyber Command has sought to disrupt the world's largest botnet, hoping to reduce its potential impact on the election," *The New York Times*, October 11, 2020; U.S. Gen. Nakasone acknowledged for the first time in December 2021 that Cyber Command had taken offensive actions against ransomware groups. "U.S. military has acted against ransomware groups, General acknowledges," *The New York Times*, December 5, 2021. A botnet is a set of computers infected by bots. A bot is a piece of malicious software that gets orders from a master. European Union Agency for Cybersecurity (ENISA), https://www.enisa.europa.eu/topics/incident-response/glossary/botnets?v2=1

259 "Canadian spy agency targeted foreign hackers to 'impose a cost' for cybercrime," *Global News*, December 6, 2021, https://globalnews.ca/news/8429008/canadian-spy-agency-targets-cybercrime/

260 See Estonia, position paper, UN Doc. A/76/136, p. 28, III.

261 "…countermeasures may be taken by the injured State, i.e., the State specifically affected by the breach, as well as third States in response to violations of obligations of an erga omnes nature or upon request by the injured State." Costa Rica, position paper, p. 5, para. 15.

262 "The question of collective countermeasures does not seem to have been fully settled in state practice and needs careful consideration. As a general observation Denmark finds that there may be instances where one State suffers a violation of an obligation owed to the international community as a whole, and where the victim State may request the assistance of other States in applying proportionate and necessary countermeasures in collective response hereto." Denmark, position paper, p. 9.

263 "…since the adoption of the ARSIWA in 2001, state practice indicates that such measures are permissible in limited circumstances, in particular in the context of violations of peremptory norms. The possibility of imposing third party or collective countermeasures in the cyber context is particularly relevant for states that may consider it necessary to respond to a malicious cyber-operation with a counter-operation, but lack the technological capacity to do so on their own." Ireland, position paper, p. 6, para. 26.

264 "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." New Zealand, position paper, p. 4, para. 22.

265 Canada, position paper, para. 37.

266 Ministre des Armées, *Droit international appliqué aux operations dans le cyberspace*, p. 8, para. 1. 1. 3.

267 Brazil, position paper, UN Doc. A/76/136, pp. 21–22, section 4.

268 Crawford, *ILC's Articles on State Responsibility*, p. 178.

269 Crawford, *ILC's Articles on State Responsibility*, p. 179, para. 3.

270 TM1 Rule 9 commentary, pp. 39–40, paras. 10–12.

271 TM1 Rule 9 commentary, p. 40, p. 11.

272 Ibid., para. 12.

273 TM2, p. 135.

274 TM2 Rule 26 commentary, p. 135, para. 1.

275 TM2 Rule 26 commentary, p. 136, para. 5.

276 Michael N. Schmitt, "Peacetime Cyber Responses and Wartime Cyber Operations under International Law: An Analytical Vade Mecum," *Harvard National Security Journal*, Vol. 8, 2017, p. 252, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3180699

277 TM2 Rule 26 commentary, pp. 135–136, para. 2.

278 TM2 Rule 26 commentary, p. 137, para. 9. The counterpart sentence in the commentary to necessity in ARSIWA is slightly different: "…it is not dependent on the prior conduct of the injured State." Crawford, *ILC's Articles on State Responsibility*, p. 178, para. 2.

279 TM2 Rule 26 commentary, p. 137, para. 6.

280 TM2 Rule 26 commentary, p. 137, para. 8.

281 TM2 Rule 7 commentary, p. 49, para. 24.

282 Sara Heathcote, "Circumstances Precluding Wrongfulness in The ILC Articles on State Responsibility: Necessity," in Crawford, Pellet, Olleson, and Parlett, eds., *Law of International Responsibility*, p. 496.

283 TM2 Rule 20 commentary, p. 116, para. 16.

284 TM2 Rule 26 commentary, p. 140, para. 18.

285 TM2 Rule 26 commentary, p. 136, para. 3.

286 Crawford, *ILC's Articles on State Responsibility*, p. 183, para. 15.

287 Heathcote, "Circumstances Precluding Wrongfulness," p. 491.

288 TM2 Rule 26 commentary, p. 141, paras. 21–22.

289 The TM2 Director's article on the topic cites no particular incidents. Louise Arimatsu and Michael N. Schmitt, "The Plea of Necessity: An Oft Overlooked Response Option to Hostile Cyber Operations," *U.S. Naval War College International Law Studies*, Vol. 97, 2021, https://digital-commons.usnwc.edu/ils/vol97/iss1/46/

290 Crawford, *ILC's Articles on State Responsibility*, p. 184.

291 TM2 Rule 26 commentary, p. 138, para. 12.

292 TM2 Rule 26 commentary, p. 139, para. 16.

293 Costa Rica, position paper, p. 5, para. 16; France, position paper, p. 5; Finland, position paper, p. 12; Italy, position paper, p. 4; Japan, position paper, UN Doc. A/76/136, p. 48; Sweden, position paper, pp. 7–8; Switzerland, position paper, A/76/136, p. 91; Remarks by Egan, in *Digest of U.S. Practice in International Law*, 2016, p. 821.

294 UN Doc. A/76/136, pp. 42–43.

295 UN Doc. A/76/136, pp. 63–64.

296 UN Doc. A/76/136, p. 73.

297 Norway, position paper, UN Doc. A/76/136, p. 73, para. 5.3.

298 TM2 Rule 26 commentary, p. 137, para. 9. The counterpart sentence in the commentary to necessity in ARSIWA is slightly different with "…it is not dependent on the prior conduct of the injured State." Crawford, *ILC's Articles on State Responsibility*, p. 178, para. 2.

299 Menno T. Kamminga, "Extraterritoriality," *Max Planck Encyclopedia of Public International Law*, September 2020, https://opil-ouplaw-com.ep.fjernadgang.kb.dk/display/10.1093/law:epil/9780199231690/law-9780199231690-e1040?rskey=LmbaIV&result=4&prd=MPIL

300 TM1 Rule 3 commentary, p. 253, para. 5.

301 TM2, p. 66.

302 TM2 Rule 11 commentary, pp. 70–71, paras. 14 and 17.

303 TM2 Rule 11 commentary, p. 69, para. 12.

304 TM2 Rule 11 commentary, pp. 69–70, para. 13

305 TM2 Rule 11 commentary, p. 70, para. 14.

306 TM2 Rule 11 commentary, p. 70, para. 15.

307 Cedric Ryngaert, "Extraterritorial Enforcement Jurisdiction in Cyberspace: Normative Shifts," *German Law Journal*, Vol. 24, 2023, pp. 540, 543, https://www.cambridge.org/core/journals/german-law-journal/article/extraterritorial-enforcement-jurisdiction-in-cyberspace-normative-shifts/3F1E5EED62283DB200D2F6026A6CE951

308 Supreme Court of Norway, Order, HR-2019-610-A, (case no. 19-010640STR-HRET), criminal case, appeal against order: Tidal Music AS v. The public prosecution authority, https://www.domstol.no/globalassets/upload/hret/decisions-in-english-translation/hr-2019-610-a.pdf

309 Ibid., para. 36.

310 Ibid., para. 58.

311 Ibid, paras. 65, 67, 69–71.

312 Ibid., para. 51.

313 Lars Bo Langsted, "Commentary: Commentary to Supreme Court Order U 2012.2614 H," *Digital Evidence and Electronic Signature Law Review*, Vol. 10, 2013, pp. 162–165, https://journals.sas.ac.uk/deeslr/article/view/2038/1975

314 TM2, Rule 11 commentary, p. 70, para. 16.

315 Court of Cassation, case nr. P.17.1229.N, 19 February 2019, *Cybercrime Judicial Monitor*, Issue 5, 2019, p. 7, para. 2, https://www.eurojust.europa.eu/sites/default/files/assets/2019_12_cjm_5_en.pdf; Ryngaert, "Extraterritorial Enforcement Jurisdiction," p. 546.

316 TM2 Rule 11 commentary, p. 70, para. 15.

317 Ibid.

318 Gary P. Corn and Robert Taylor, "Sovereignty in the Age of Cyber," *American Journal of International Law Unbound*, Vol. 111, 2017, p. 211, https://www.cambridge.org/core/journals/american-journal-of-international-law/article/sovereignty-in-the-age-of-cyber/02314DFCFE00BC901C95FA6036F8CC70

319 As for Operation Glowing Symphony (OGS), see Michael Warner, "US Cyber Command's First Decade," in Jack Goldsmith, ed., *The United States' Defend Forward Cyber Strategy: A Comprehensive Legal Assessment*, Oxford University Press, 2022, p. 50 et seq.

320 International Institute for Strategic Studies, ed., *Cyber Capabilities and National Power: A Net Assessment*, 2021, p. 52, https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/cyber-power-report/cyber-capabilities-and-national-power---a-net-assessment___.pdf

321 Canada, position paper, para. 15.

322 Ryngaert, "Extraterritorial Enforcement Jurisdiction," pp. 542–543.

323 "[o]pinion is divided as to what qualifies as exercising investigative powers in a cross-border context and when it is permissible without a legal basis founded in a treaty. In cyberspace too, countries' practices differ in their practical approaches to the principle of sovereignty in relation to criminal investigations." The Netherlands, position paper, UN Doc. A/76/136, pp. 56–57.

324 "Germany recognizes that due to the high degree of cross-border interconnectedness of cyber infrastructures, a State's exercise of its jurisdiction may have unavoidable and immediate repercussions for the cyber infrastructure of

other States." In footnote 61 at the end of the sentence: "For example, restrictive regulatory or enforcement activities regarding important internet nodes in the territory of one State may seriously impair the functioning of networks of other States." Germany, position paper, A/76/136, p. 32.

325 "13. … the application of the rule of territorial sovereignty in cyberspace must take into account some critical features that distinguish cyberspace from the physical realm. In particular: i) cyberspace contains a virtual element which has no clear territorial link; ii) cyber activity may involve cyber infrastructure operating simultaneously in multiple territories and diffuse jurisdictions;" and "26 …The circumstances in which states exercise jurisdiction, through cyber means, over individuals outside their territory is currently unsettled and would benefit from further discussion in multilateral fora." New Zealand, position paper, pp. 2, 4.

326 Council of Europe, https://www.coe.int/en/web/cybercrime/second-additional-protocol

327 Ryngaert, "Extraterritorial Enforcement Jurisdiction," p. 547.

328 UN Doc. A/AC.291/22. Article 4 [Protection of sovereignty], paragraph 2: "Nothing in this Convention shall entitle a State Party to undertake in the territory of another State the exercise of jurisdiction and performance of functions that are reserved exclusively for the authorities of that other State by its domestic law."

329 TM1, p. 106.

330 The ICRC, International Humanitarian Law Database, Article 49 (1) of API [Definition of attacks and scope of application], https://ihl-databases.icrc.org/en/ihl-treaties/api-1977/article-49?activeTab=default

331 TM2, p. 415.

332 TM1 Rule 30 commentary, pp. 106–107, para. 3; TM2 Rule 92 commentary, pp. 415–416, para. 3.

333 TM1 Rule 30 commentary, p. 107, para. 4; TM2 Rule 92 commentary, p. 416, para. 4.

334 TM1 Rule 30 commentary, pp. 107–108, para. 6; TM2 Rule 92 commentary, p. 416, para. 6.

335 TM1 Rule 30 commentary, pp. 108–109, para. 10; TM2 Rule 92 commentary, p. 417, para. 10.

336 TM1 Rule 30 commentary, p. 109, para. 10; TM2 Rul3 92 commentary, pp. 417–418, para. 11.

337 TM1 Rule 30 commentary, p. 109, para. 11; TM2 Rule 92 commentary, p. 418, para. 12.

338 Laurent Gisel, Tilman Rodenhäuser, and Knut Dörmann, "Twenty Years On: International Humanitarian Law and the Protection of Civilians against the Effects of Cyber Operations during Armed Conflicts," *International Review of*

the Red Cross, No. 913, 2021, pp. 313–314, https://international-review.icrc.org/articles/twenty-years-international-humanitarian-law-and-protection-civilians-against-effects-cyber-913

339 TM1 Rule 30 commentary, p. 109, para. 12; TM2 Rule 92 commentary, p. 418, para. 13.

340 *Cyberscoop* staff, "Victor Zhora on Cataloging Cyberwar Crime Evidence against Russian Hackers Targeting Ukraine," *Cyberscoop*, August 9, 2023, https://cyberscoop.com/victor-zhora-cyberwar-crime-ukraine-russia/

341 TM1 Introduction, p. 5.

342 Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," *Wired*, August 22, 2018, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

343 Ibid.

344 TM2 Rule 92 commentary, p. 416, para. 5.

345 Morgan Schneer, "Accountability for NotPetya: Why the International Criminal Court Can, and Should, Prosecute the Perpetrators of the NotPetya Cyber Attack as a War Crime," ICCForum.com, March 4, 2022, https://iccforum.com/forum/permalink/131/38972

346 It is widely known that due to budget shortages throughout Ukraine, victimized computers were rarely replaced with new ones.

347 Greenberg, "The Untold Story of NotPetya."

348 CISA, "Update: Destructive Malware Targeting Organizations in Ukraine," April 28, 2022, https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-057a

349 Karim A. A. Khan KC, "Technology Will Not Exceed Our Humanity," *Digital Front Lines*, August 20, 2023, https://digitalfrontlines.io/2023/08/20/technology-will-not-exceed-our-humanity/

350 *Cyberscoop*, "Victor Zhora on Cataloging Cyberwar Crime Evidence."

351 Israel, position paper, p. 400. The next paragraph continues: "However, if an impediment to functionality is caused by physical damage, or when an act causing the loss of functionality is a link in a chain of the expected physical damage, that act may amount to an attack. For example, if a cyber operation is intended to shut down electricity in a military airfield, and as a result is expected to cause the crash of a military aircraft—that operation may constitute an attack (subject, of course, to the additional elements for attacks under LOAC)" (Ibid., pp. 400–401). But this part does not involve the issue of interference with the functionality discussed by TM experts.

352 Ireland, position paper, pp. 7–8.

353 Costa Rica, position paper, p. 13.

354 France, position paper, pp. 11–12.

355 Italy, position paper, pp. 9–10.

356 New Zealand, position paper, p. 4.

357 Pakistan, position paper, p. 4. More specifically, Pakistan argues that cyber-attack under IHL includes "[a]ny attempt to delete, destroy and manipulate the data essential for the smooth functioning of the critical civilian infrastructure may impair its operations."

358 Japan, position paper, UN Doc. A/76/136, p. 50.

359 Germany, position paper, pp. 36–37.

360 Canada, position paper, para. 49.

361 TM1 Rule 10 commentary, p. 45, para. 10.

362 TM2 Rule 66 commentary, p. 313, para. 2.

363 TM2 Rule 26 commentary, p. 136, para. 3.

364 TM1 Rule 9 commentary, p. 40, para. 11.

365 TM Director Schmitt admits that "[t]he 'inherently governmental function' concept lacks granularity." Schmitt, "'Virtual' Disenfranchisement," p. 45.

366 TM2 Rule 26 commentary, p. 137, paras. 6 and 8.

367 TM2 Rule 7 commentary, p. 49, para. 24.

368 TM2 Rule 7 commentary, p. 50, para. 28.

369 TM2 Rule 23 commentary, p. 130, para. 12.

370 TM2 Rule 20 commentary p. 114, para. 10.

371 TM2 Rule 23 commentary, p. 130, para. 12.

372 TM2 Rule 26 commentary, p. 141, paras. 21–22.

373 Samuli Haataja, "Cyber Operations and Collective Countermeasures under International Law," *Journal of Conflict and Security Law*, Vol. 25, 2020, p. 47.

374 Sicilianos, "Countermeasures in Response to Grave Violations," pp. 1139–1140.

375 Ibid., p. 1142.