UNIVERSITY OF AMSTERDAM

UvA-DARE (Digital Academic Repository)

Cyber-attacks and the right of self-defense

a case study of the Netherlands

Oorsprong, F.; Ducheine, P.; Pijpers, P.

DOI
10.1080/25741292.2023.2179955

Publication date
2023

Document Version
Final published version

Published in
Policy Design and Practice

License
CC BY

Link to publication

Citation for published version (APA):
Oorsprong, F., Ducheine, P., & Pijpers, P. (2023). Cyber-attacks and the right of self-defense: a case study of the Netherlands. *Policy Design and Practice*, *6*(2), 217-239. https://doi.org/10.1080/25741292.2023.2179955

General rights
It is not permitted to download or to forward/distribute the text or part of it without the consent of the author(s) and/or copyright holder(s), other than for strictly personal, individual use, unless the work is under an open content license (like Creative Commons).

Disclaimer/Complaints regulations
If you believe that digital publication of certain material infringes any of your rights or (privacy) interests, please let the Library know, stating your reasons. In case of a legitimate complaint, the Library will make the material inaccessible and/or remove it from the website. Please Ask the Library: https://uba.uva.nl/en/contact, or a letter to: Library of the University of Amsterdam, Secretariat, P.O. Box 19185, 1000 GD Amsterdam, The Netherlands. You will be contacted as soon as possible.

UvA-DARE is a service provided by the library of the University of Amsterdam (https://dare.uva.nl)

Download date:15 Nov 2026

POLICY DESIGN AND PRACTICE
2023, VOL. 6, NO. 2, 217–239
https://doi.org/10.1080/25741292.2023.2179955

Routledge
Taylor & Francis Group

OPEN ACCESS Check for updates

Cyber-attacks and the right of self-defense: a case study of the Netherlands

Ferry Oorsprong[a], Paul Ducheine[b] and Peter Pijpers[a]

[a]Faculty of Military Sciences, Netherlands Defense Academy, Breda, the Netherlands; [b]Faculty of Law, University of Amsterdam, Amsterdam, the Netherlands

ABSTRACT

Whilst Article 51 of the UN Charter as a rule indicates that an "armed attack" may trigger a State's right of self-defense, the actual purport of armed attack remains a matter of interpretation and qualification. To improve the notion of the rule on self-defense and contribute to the *jus ad bellum*, more clarification as to what constitutes an armed attack in cyberspace is necessary. Therefore, policy norms—regarding when cyber-attacks reach the threshold of an armed attack—could guide State behavior. On the one hand, these policy norms could be used in the political decision-making processes for States that consider initiating cyber-attacks. On the other, they could help victim States in their decision-making processes in response to grave cyber-attacks. The aim of the paper is to propose a tangible guideline that outlines when cyber-attacks—perpetrated solely in or through cyberspace and not in conjunction with conventional military attacks—can qualify as an armed attack. By assessing the positions of States and leading academic opinions regarding the qualification of cyber-attacks as armed attacks, and applying international and interdisciplinary policy documents to transfer the legal debate into tangible options, a policy framework is deduced that can serve as a baseline for international cyber norms. This framework distinguishes three separate categories of armed attack in cyberspace, each with their own distinctive levels to determine when a cyber-attack can qualify as an armed attack. These absolute levels are tailored for the Netherlands but could also be suitable for other States when transferred to percentages of the gross national/domestic product and the population size.

ARTICLE HISTORY
Received 31 March 2022
Accepted 7 December 2022

KEYWORDS
Armed attack; self-defense; cyberspace; threshold; Article 51; UN Charter

1. Introduction

> *"Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken the measures necessary to maintain international peace and security."*[1]

CONTACT Ferry Oorsprong fme.oorsprong@mindef.nl Faculty of Military Sciences, Netherlands Defense Academy, Breda, Netherlands

© 2023 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group.
This is an Open Access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Whilst Article 51 of the UN Charter indicates that an "armed attack" may trigger a State's inherent right of individual or collective self-defense, the purport of armed attack remains a matter of both interpretation and qualification.[2] Prior to 9/11, the traditional interpretation of an armed attack—as referred to in Article 51—relied on the transnational use of military force by State actors on a "relatively large" *scale* with "substantial" *effect* (Gill 2015; Gill and Ducheine 2013; Randelzhofer 1994). Since 9/11, however, a more modern interpretation arose, accepting the fact that also unorthodox uses of force by non-State actors could qualify as such (Gill and Tibori-Szabó 2019). Fourteen years later, this interpretation was expressed again when France invoked the mutual defense clause of Article 42(7) of the Treaty on European Union—based on Article 51 of the UN Charter—after the Bataclan terrorist attacks in Paris (Boddens Hosang and Ducheine 2020). In the same vein, actions carried out in cyberspace have caused the impetus for further debate regarding whether and when digital attacks (or incursions)—conducted solely in (or through) cyberspace and not in conjunction with conventional uses of force and attacks—can qualify as an armed attack (Boothby et al. 2012). Although scholars (Schmitt 2017), international organizations (UN GGE 2015 Report 2015), coalitions (UN General Assembly 2021), and even States (the Netherlands included) (Ministry of Foreign Affairs 2019) have (to some extent) expressed legal opinions in this respect, unfortunately, the debate has yet to reach a conclusion.

To improve the notion of self-defense and contribute to the *jus ad bellum* (international law on the use of transnational force), more clarification as to what constitutes an armed attack in cyberspace is necessary. It is, however, rather unlikely that additional binding legal norms will be drafted regarding this topic (Schmitt 2020). Therefore, non-binding norms or guidance—regarding when cyber-attacks reach the threshold of an armed attack—could be conducive to guide State behavior.[3] While rules are legally binding to all States (when part of customary international law) or to those States that are part of a specific treaty, their application can face ambiguity. Norms, on the other hand, are indicia providing additional points of reference for interpreting and applying existing legislation. Besides the fact that such norms would serve as the start of a form of (international) law making (Mačák 2017), in which, primarily, States incrementally reach an agreement regarding the armed attack-threshold in cyberspace and its impact on self-defense, the results would be 2-fold: one of particular relevance for the author of the attack, and another for the addressee, i.e. the victim of the attack. First, the armed attack-threshold, when applied in cyberspace, could be used in the political decision-making processes for States considering initiating a cyber-attack. It may be expected that States—the authors of cyber-attacks—will (a) try to abide by the *jus ad bellum*, (b) pay respect to the prohibition of the use of force as referred to in Article 2(4) of the UN Charter, and (c) be aware of the consequences if cyber-attacks of a certain *scale* and *effect* qualify as an armed attack in terms of Article 51 of the UN Charter. This relates to the second result: clarity on the parameters regarding the armed attack-threshold in cyberspace would help victim States in their decision-making processes in response to cyber-attacks with a grave impact. If the armed attack-threshold would indeed be reached, it then offers the victim State a legal base in international law for the use of transnational force—i.e. self-defense—in response to that attack (Gill 2015).

The main aim of this paper is to propose a tangible guideline that outlines when cyber-attacks—conducted solely in (or through) cyberspace and not in conjunction with conventional military attacks—qualify as an armed attack. The center of attention will be cyber-attacks directed against civilian (i.e. nonmilitary) targets. In order to do so, section 2 will contain a brief appreciation of the traditional interpretation of an armed attack, with a focus on explaining why judging the *scale* and *effect* is crucial for its identification. Section 3 is a survey of positions of States (*opinio juris*) and leading academic opinions regarding the application of international law in cyberspace, specifically aimed at the qualification of cyber-attacks as armed attacks. This survey confirms the applicability of international law in cyberspace and provides some specific examples of potential armed attacks in cyberspace. Section 4 is key to this contribution, as it transfers the legal debate into tangible options by applying policy documents from other States and disciplines. To enable that cross-fertilization, this section first analyses which type(s) of cyber-attacks is/are eligible to qualify as an armed attack, followed by the analysis of international and interdisciplinary polities in search of tangible indicators for the armed attack-threshold that can be used in cyberspace. This process, based on desk research, results in eleven cyber-attack scenarios that could (theoretically) qualify as an armed attack.[4] These scenarios (as summarized in Appendix A) were used to conduct structured interviews to collect verbal statements from leading cyber experts from the Netherlands' ministries of (a) Foreign Affairs, (b) Defense, and (c) Justice and Security regarding when these theoretically identified potential armed attacks in cyberspace would actually reach the armed attack-threshold in practice and, therewith, trigger the Netherlands' right of self-defense. The choice was made to interview two legal experts (focussing on the legal eligibility), two policy experts (focussing on the strategic credibility) and one operational expert (focussing on the technical feasibility). During five interviews in total, the experts were asked (as if they were advising their minister) to judge whether and how each cyber-attack scenario could reach the necessary (*scale* and *effect*) threshold for triggering the Netherlands' right of self-defense. Section 5, eventually, presents the results of the field research and suggests a policy framework regarding the *scale* and *effect* of armed attacks in cyberspace that can serve as a baseline for international norms or guidance regarding the armed attack-threshold. This policy framework distinguishes three separate cyber-attack categories, each with their own tangible levels to determine if and when they qualify as an armed attack. For now, these levels are tailored for the Netherlands in absolute numbers, but when transferred to percentages of the gross national/domestic product and the population size, they could perhaps be suitable for other States as well. The paper will end with some concluding reflections.

2. Armed attack and the lacking ability to judge *scale* and *effect*

Self-defense in response to an armed attack, as referred to in i.a. Article 51 of the UN Charter, is one of the legal exceptions to the prohibition of the transboundary use of force, as laid down in Article 2(4) of the UN Charter.[5] Since the prohibition of the use of force has the status of peremptory norm or *jus cogens*,[6] it might be surprising that the UN Charter lacks a definition of both "use of force" and "armed attack" (Dinnis

2012, 77; Kerschischnig 2012, 111). Therefore, in practice, the armed attack-standard requires an interpretation based on the case at hand, resulting in the fact that expert opinions—regarding the purport of armed attack—have differed to this day (Ruys 2010, 1).

Starting with the term force, the UN Charter uses "force" with and without the adjective "armed." The assumption in this paper is that when the UN Charter uses "force," it encapsulates "armed force." This was epitomized by the rejection of a Brazilian amendment to also prohibit "the threat or use of economic measures" during the *travaux préparatoires* at the San Francisco Conference in 1945 (UNIO 1945, 609; Roscini 2014, 45–46).[7] This rejection implies that the drafters of the UN Charter did not intend to expand the interpretation of force beyond armed force (Roscini 2014, 45). With regard to the scope of use of force, which does not coincide with the scope of armed attack (Randelzhofer 1994, 663), not every use of force equals an armed attack.[8] This understanding is reflected in the *Nicaragua* Case in which the International Court of Justice (ICJ) mentioned that "armed attacks form a subset of the term force in Article 2(4)" (Dinnis 2012, 77). In the same *Nicaragua* Case, the ICJ provided another indication of how the term armed attack should be understood by asserting the necessity "to distinguish the most grave forms of the use of force (those constituting an armed attack) from other less grave forms" (Ruys 2010, 140; ICJ 1986, para 191, 101). This necessity corresponds with academic opinions implying that an armed attack only exists in case of a "reasonably significant" *use of force* on a relatively large *scale* with substantial *effect* (Randelzhofer 1994, 669; Gill 2015, 216). Paragraph 195 of the *Nicaragua* Case, in which the ICJ stated that "the difference between armed attacks and less grave forms of the use of force is primarily one of scale and effects," substantiates this approach (Ruys 2010, 140). However, the crucial and remaining question to be answered is when the *scale* and *effect* of the use of force are considered relatively large and substantial, and how this should be clarified and assessed.

According to Yoram Dinstein "a use of force not involving loss of life or significant destruction of property falls short of an armed attack" (Dinstein 2013, 279). This could imply that "loss of life" and "*significant* destruction of property" are criteria for an armed attack. On the other hand, Tom Ruys argues that customary practice suggests that even small-scale operations can qualify as an armed attack if it concerns "bombings, artillery, naval or aerial attacks" resulting in, or capable of resulting in "destruction of property or loss of lives" (Ruys 2010, 155). Still, for operations without these specific (kinetic) characteristics, appraising the *scale* and *effect* as relatively large and substantial would remain necessary in order for the *use of force* to be "reasonably significant" and qualify as an armed attack.

Overall, this implies that judging the *scale* and *effect* is crucial for identifying an armed attack. However, to this day, no tangible criteria have been defined for that purpose in international law (i.e. the *jus ad bellum*).

3. The application of international law for qualifying cyber-attacks as armed attacks

Although international law does not provide tangible criteria regarding the application of the armed attack-standard, when analyzing the extent to which cyber-attacks

can qualify as an armed attack, other sources can provide additional guidance. Therefore, this section will first elaborate on leading academic opinions, followed by the positions expressed by States.[9]

3.1. Leading academic opinions

At the invitation of the North Atlantic Treaty Organization (NATO) Cooperative Cyber Defence Center of Excellence (CCD COE), an International Group of Experts (IGE) drafted the Tallinn Manuals. The first edition, that covered the applicability of international law to "cyber warfare," was followed by the 2.0 version that focused on how international law applies more broadly to "cyber operations" (Schmitt 2013b, 1–4). Although the Tallinn Manuals are no official legal documents, the leading academic experts gathered in the IGE unanimously stated that existing international law applies to cyberspace (Schmitt 2017, 3; Schmitt 2013b, 24), and is applicable to cyber operations (Schmitt 2017, 3).

Regarding armed attacks, the IGE also unanimously agreed that some cyber operations can be "sufficiently grave" to qualify as an armed attack, which is in accordance with the ICJ's Nuclear Weapons advisory opinion arguing that "the choice of means of attack is immaterial to the issue of whether an operation qualifies as an armed attack" (ICJ 1996; Schmitt 2017, 340, Rule 71, para. 4). Dinstein supports the IGE's opinion by stating that "the legal principles of the customary *jus ad bellum* remain intact whether the armed attack is kinetic or cyber" (Dinstein 2013, 280). Dinstein has also stated that "all armed attacks (justifying individual and collective self-defense in response, pursuant to Article 51) must be subject to the same criteria, whatever weapon is resorted to" (Roscini 2014, viii). However, the remaining crucial question—again—is how and when cyber-attacks can be judged as "sufficiently grave." In this respect, the IGE took notice of the ICJ decision in the *Nicaragua* Case stating that "scale and effects are to be considered when determining whether particular actions amount to an armed attack" (Schmitt 2017, 330, Rule 69, para. 1).

Unfortunately, existing international law provides little tangible criteria to judge *scale* and *effect* (ICJ 2003, para 72, 195–196; ICJ 2005, para 143, 222; UN 1974). Nevertheless, the IGE agreed that "a cyber operation that seriously injures or kills a number of persons or that causes significant damage to, or destruction of, property" meets the threshold of an armed attack (Schmitt 2017, 341, Rule 71, para. 8). Moreover, Marco Roscini—one of the IGE legal peer reviewers (Schmitt 2017, xvii)—concluded that "the use of any device […] which results in a considerable loss of life and/or extensive destruction of property must be deemed to fulfill the conditions of an armed attack" (Roscini 2014, 71). One specific example was unanimously considered to qualify as an armed attack: a cyber operation conducted to assassinate a foreign head of state while abroad (Schmitt 2015, 1123; Schmitt 2017, 346, Rule 71, para. 22). However, broad criteria like *seriously*, *a number of*, *significant*, *considerable* and *extensive* contain no clear parameters. Moreover, how should a cyber operation be dealt with that does not kill the head of State, but the CEO of the largest State-owned corporation instead? For that question, the IGE was unable to define a "bright-line rule" (Schmitt 2017, 346, Rule 71, para. 22).

Other cases are even less clear, especially if cyber operations do not directly result in injury, death, damage or destruction (Schmitt 2012, 288; Schmitt 2017, 342, Rule 71, para. 12). The classic scenario in this non-kinetic context is a cyber operation against "a major international stock exchange that causes the market to crash" (Schmitt 2017, 343, Rule 71, para. 12). The IGE reached no consensus in this case, but—in the absence of a "conclusive definitional threshold"—States should be "highly sensitive to the international community's probable assessment" when judging the *scale* and *effect* of cyber operations (Schmitt 2017, 333, Rule 69, para. 8).[10] The positions of States, addressed in the next paragraph, will help estimating this "international community's probable assessment" (Schmitt 2017, 333, Rule 69, para. 8).

3.2. Positions of states

During the second UN Open-Ended Working Group (OEWG) in February 2020, open to all 193 UN members, but also earlier during the two UN Groups of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security in 2013 and 2015, States—including Russia and China (UN GGE 2015 Report 2015)—confirmed the applicability of international law in cyberspace, the UN Charter inclusive (Tolppa 2020; Broeders 2021, 1–2). Although, to this day, no State has explicitly labeled a cyber-attack launched against it as an armed attack (Ministère des Armées 2019, 8), several States have presented more specific views regarding this issue. In the search for legal positions of States regarding the qualification of cyber-attacks as armed attacks, this paper focused on statements from the United Kingdom (UK), France, Estonia and the Netherlands, due to their firm articulation concerning this topic.[11]

Each of these States confirmed that a cyber-attack may reach the threshold of an armed attack (derived from Attorney General's Office 2018; Ministère des Armées 2019; Sits 2019; Minister of Foreign Affairs 2019, 8). Moreover, inspired by the traditional approach for determining the attributes of an armed attack, all four States are willing to qualify cyber-attacks as an armed attack if their consequences are comparable to those of kinetic armed attacks (Attorney General's Office 2018; Ministère des Armées 2019, 8; Sits 2019; Minister of Foreign Affairs 2019, 8–9; Schmitt 2012, 288). Additionally, there are some particular positions of individual States. The UK states that (a) "if a hostile state interferes with the operation of one of our nuclear reactors, resulting in widespread loss of life, the fact that the act is carried out by way of a cyber operation does not prevent it from being viewed as an unlawful use of force or an armed attack against us," (b) "if it would be a breach of international law to bomb an air traffic control tower with the effect of downing civilian aircraft, then it will be a breach of international law to use a hostile cyber operation to disable air traffic control systems which results in the same, ultimately lethal, effects" and (c) "acts like the targeting of essential medial services are no less prohibited interventions, or even armed attacks, when they are committed by cyber means" (Attorney General's Office 2018). According to France, a cyber-attack could be categorized as an armed attack if it causes "substantial loss of life or significant physical or economic damage"

(Schmitt 2019a). That would be the case if an operation in cyberspace "caused a failure of critical infrastructure with significant consequences or consequences liable to paralyze whole swathes of the country's activity, trigger technological or ecological disasters and claim numerous victims" (Ministère des Armées 2019, 8). Estonia considers a cyber operation "which for example, targets digital infrastructure or services necessary for the functioning of society" eligible for qualification. Moreover, Estonia believes that "growing digitalization of our societies and services can also lower the threshold for harmful effects" (Sits 2019).

The Netherlands' legal opinion explicitly articulates that the qualification of a cyber-attack as an armed attack "depends on the scale and effects of the incident in question" (Minister of Foreign Affairs 2019, 8–9). It also articulates that a cyber-attack must have a cross-border character to be able to qualify as an armed attack (Parliamentary Papers II 2019–2020, 33 694, nr 47 2019). Moreover, a cyber-attack "that has comparable consequences to an armed attack (fatalities, damage and destruction) can justify a response with cyber weapons or conventional weapons (…)" (Ministry of Foreign Affairs 2019). The Government of the Netherlands, therefore, endorses the finding of the CAVV and the AIV Advisory Report on Cyber Warfare. The report stated that "a serious, organized cyber-attack on essential functions of the state could conceivably be qualified as an armed attack within the purpose and intent of Article 51 of the UN Charter if it could or did lead to serious disruption of the functioning of the state or serious and long-lasting consequences for the stability of the state" (AIV/CAVV 2011, 21).

Inspired by examples from the same report, which also explicitly included "an attack on the entire military communication and command network that makes it impossible to deploy the armed forces" (AIV/CAVV 2011, 21), the (then) Netherlands' minister of Defense suggested in her keynote address, marking the first anniversary of the Tallinn Manual 2.0 on the 20th of June 2018, that "if a cyber-attack targets the *entire Dutch financial system*, or if it prevents the government from carrying out essential tasks such as *policing* or *taxation*… it would qualify as an armed attack and thus trigger a state's right to defend itself, even by force" (Bijleveld 2018, 45). Although there is no international consensus regarding cyber-attacks with a relatively large *scale* and substantial *effect* that do not cause fatalities, physical damage or destruction (Parliamentary Papers II 2019–2020, 33 694, nr 57 2019), this view was echoed by Michael Schmitt when he analyzed these Netherlands' statements (Schmitt 2019b).

4. In search of a threshold: cross-fertilization to assess eligible cyber-attacks

Although the previous section provided some potential examples, a list of "ready-made" armed attacks in cyberspace cannot be composed at this point. Therefore, this section aims to transfer the legal debate into policy options. In order to take this crucial step, the first paragraph will analyze which type(s) of cyber-attack is/are considered eligible for armed attack-qualification. In the second paragraph, international and interdisciplinary policy documents will be introduced to enable us to provide

more granularity than academics or (representatives of) States have (openly) done so far, as to when these eligible cyber-attacks could reach the threshold of an armed attack.

4.1. Analyzing the eligibility of cyber-attacks

In principle, cyber-attacks between States—without taking enabling attacks in support of conventional attacks into account—can be categorized in three different types: "cyber espionage,"[12] "manipulation of the information environment," and "disruption, degradation or destruction of core security assets" (Whyte and Mazanec 2019, 100–101).[13] For each type, an analysis will take place to determine whether it is eligible to qualify as an armed attack.

Due to the large scale at which modern "cyber espionage"—also referred to as information exfiltration—takes place, this *first* type has become a real concern and a kind of intrusion that is too disturbing and too big to ignore (Maurer 2018, 56). An illustrative example is the blueprint information for the F-35 fighter aircraft that—according to the Snowden Leaks—was among the more than 50 TB of information that China stole from the United States (US) government in a years-long theft operation (Valeriano and Maness 2015, 95; Whyte and Mazanec 2019, 120). However, even the most relentless "close access cyber espionage operations" (Schmitt 2017, 171, Rule 32, para. 8 + 9) would not be graded as "cyber warfare" (Ducheine and Pijpers 2021, 276), regardless of their severity or the method employed (Schmitt 2017, 171, Rule 32, para. 8). In fact, cyber espionage is to be considered as (merely) an intelligence or counter-intelligence operation (Ducheine and Pijpers 2021, 287–288). Therefore, cyber espionage operations do not violate Article 2(4) and will not be considered eligible for qualification as an armed attack.

With regard to the *second* cyber-attack type, an illustrative example of "manipulation of the information environment" is the way Russia and (perhaps even more impressively) Cambridge Analytica (contracted by the Republican Party) displayed their methods during the US elections in 2016. Especially the combined use of social media and big data to massively target and influence individual voters, demonstrated that modern techniques can manipulate the information environment and harm the democratic integrity of Western countries (Hakim and Rosenberg 2018; Amer and Noujaim 2019; Pijpers and Ducheine 2020; Pijpers 2022). Moreover, while manipulation of the information environment is not an obvious expression of force, it could be regarded as a psychological instrument or "weapon". Nevertheless, despite its harmfulness, both the UK and the Netherlands have explicitly designated "manipulating electoral systems" and "altering election outcomes" as (merely) a potential breach of the nonintervention principle (Attorney General's Office 2018; Minister of Foreign Affairs 2019, 6–7). Therefore, for the purpose of this research in which the authors focus on the Netherlands' right of self-defense, it does not amount to a violation of the prohibition of the use of force and is, thus, not considered eligible to qualify as an armed attack, regardless of its *scale* and *effect*.

The *third* type refers to "disruption, degradation or destruction of core security assets." The most straightforward analogy regarding the qualification of cyber-attacks

as an armed attack,[14] is when cyber-attacks create effects comparable to traditional kinetic weapons. A cyber-attack directed at critical infrastructure, including a nuclear powerplant to trigger a meltdown, or the system control station of a dam (upstream a populated area) could arguably fall in that category (Gill and Ducheine 2013, 444). The possibility of this qualification would especially, but perhaps not exclusively, arise if "loss of life or significant destruction of property" are involved (Dinstein 2013, 279). Therefore, in this paper, "disruption, degradation or destruction of core security assets" is the type of cyber-attack that is considered eligible for qualification as an armed attack (Schmitt 2018, 66).

4.2. Applying international and interdisciplinary policy documents

France and the UK have both developed a cyber-attack categorization system. While France only briefly describes the highest level as "extremely urgent with an extreme impact," it explicitly states that this level (Level 5: Emergency) is eligible for qualifying as an armed attack as referred to in Article 51 of the UN Charter (see Appendix B) (Secrétariat Général de la Défense et de la Sécurité Nationale 2018, 80). The UK also hints toward an armed attack by describing extensively that the highest level (Category 1: National cyber emergency) concerns a "cyber-attack which causes sustained disruption of UK essential services or affects UK national security, leading to severe economic or social consequences or to loss of life," but does not explicitly refer to it (see Appendix C) (National Cyber Security Centre 2018).

The Netherlands, in turn, has no cyber-attack categorization system, but the Netherlands' Ministry of Justice and Security did define so-called Category A (the highest level) vital processes (see Appendix D) (Nationaal Coördinator Terrorismebestrijding en Veiligheid 2020). These "core security assets" that can be disrupted, degraded or destructed by cyber-attacks can be grouped as *production, storage and processing of nuclear material* (leading to a nuclear disaster), *production, distribution and transport of electricity, gas and oil* (leading to the unavailability of electricity or other forms of energy), *water barriers* (leading to catastrophic floods), and *clean water supply* (leading to the unavailability of fresh water). Moreover, the Netherlands also defined several Category B vital processes (see Appendix D) (Nationaal Coördinator Terrorismebestrijding en Veiligheid 2020), some of which are (at least implicitly) included in the positions of States as described in paragraph 3.2.: *internet itself* (disabling the digital infrastructure or services necessary for the functioning of society), *air traffic control* (leading to air disasters), *large-scale production/-processing and/or storage of (petro)chemical substances* (leading to an "ecological disaster"), *financial systems* (including government processes for "taxation"), *communications networks* (necessary for "policing"), and *military capacity* (making it impossible to deploy the armed forces).

Building on the eligibility of cyber-attacks "disrupting, degrading or destructing core security assets" and the French (and implicitly also the British) principle that cyber-attacks belonging to the highest (emergency) category could (potentially) qualify as an armed attack, the suggestion arises that the Netherlands could consider cyber-attacks conducted against its most vital (so-called Category A) processes eligible

for armed attack-qualification. Moreover, since some cyber-attacks against Category B vital processes are (at least implicitly) included in the positions of States, their eligibility for armed attack-qualification should not be neglected. Therefore, it is suggested in this paper that the Netherlands could take cyber-attacks—authored by another State—against both Category A and (at least some) Category B vital processes into account as potential armed attacks.

What makes this suggestion so useful, is the fact that each category incorporates officially defined specific levels regarding the (minimum) expected effects in case of their "disruption, degradation or destruction." In search of a tangible guideline for the Netherlands' armed attack-threshold, these levels could provide a distinct indication with regard to when the right of self-defense would be triggered. In other words, even though the levels for the Netherlands' Category A and B vital processes were not intended for categorizing cyber-attacks (Nationaal Coördinator Terrorismebestrijding en Veiligheid 2020), they could help to judge if a cyber operation *seriously* injures or kills *enough* persons, or causes *significant* damage to, or destruction of, property. To be more specific, for the Netherlands, the necessary threshold for a cyber-attack to be severe enough in *scale* and *effect* and, thus, qualify as an armed attack, could lie somewhere in the bandwidth between the levels defined for Category A and the levels defined for Category B. In concrete terms, this would imply that a "disruption, degradation or destruction of core security assets" should cause either: (a) a *physical damage* of 1000–10,000 people dead, seriously injured or chronically sick, (b) a *societal damage* of 100,000–1,000,000 people with serious societal survivability problems, or (c) an *economic damage* of 5,000,000,000–50,000,000,000 euros (see Appendix D) (Nationaal Coördinator Terrorismebestrijding en Veiligheid 2020).

When referring to an acknowledged armed attack (the 9/11 terrorist attacks in 2001), ample support is provided for the armed attack-thresholds suggested above. For instance, the number of fatalities (2977) is inside the suggested bandwidth (Amadeo 2020). Moreover, the most direct economic damage—taking the World Trade Center buildings into account, including computers, furniture, cars, utilities, the subway system and other buildings, as well as the costs for treating injuries and cleaning up the area—was 31,000,000,000 dollars, also inside the bandwidth (Amadeo 2020).

With regard to "core security assets" in the form of *heads of State*, none of the positions of States included cyber-attacks resulting in their assassination as a potential armed attack. Also, the head of State is not defined as a Netherlands' vital "process." However, as stated in paragraph 3.1., the IGE *unanimously* regarded this a specific example to qualify as an armed attack (Schmitt 2017, 346, Rule 71, para. 22). Therefore, it was (theoretically) identified as an additional cyber-attack scenario, eligible for armed attack-qualification.

5. Policy framework regarding the *scale* and *effect* of armed attacks in cyberspace

Based on the legal appreciation of *scale* and *effect*—with regard to armed attack—by States and leading academics, and the assessment of French, British and Netherlands'

policy documents, an effort was made to establish a categorization of cyber-attacks, along with tangible thresholds for each category. Building upon the ten cyber-attack scenarios (against nonmilitary targets) that could (theoretically) qualify as an armed attack if their *scale* and *effect* would reach the suggested bandwidths, interviews were conducted with five leading Dutch cyber experts, including two legal experts; one working for the Ministry of Foreign Affairs and one working for the Ministry of Defense. With a focus on the legal *eligibility*, particularly these two experts were asked—as if they were advising their minister—to assess when these cyber-attack scenarios would reach the armed attack-threshold in practice, triggering the Netherlands' right of self-defense.[15]

Analyzing their expert judgements led to three categories of armed attack in cyberspace: (I) *comparable* to kinetic attacks, *directly* leading to *physical damage*, (II) *comparable* to kinetic attacks, *indirectly* leading to *physical damage*, and (III) *not comparable* to kinetic attacks, leading to *societal disruption*. Each category is addressed in a separate paragraph hereafter by explaining what criteria contribute to their qualification.

Moreover, two general guidelines—derived from these three categories and the contributing criteria suggested in the next three paragraphs—can be identified. First, the necessary level of proof increases when the self-evident nature of the cyber-attack decreases. This means that the less direct the harmful effects are, the more precise they have to be documented and demonstrated,[16] and the higher the level of evidence is for qualifying as an armed attack. Secondly, not all contributing criteria are equally important for armed attack qualification. With regard to the suggested thresholds, *physical damage* is considered most important.

5.1. Contributing criteria for cyber-attacks comparable to kinetic attacks, directly leading to physical damage

Identification of this first category is based on the similarities between the scenarios that comprised disruption, degradation or destruction of *production, storage and processing of nuclear material* (leading to a nuclear disaster), *water barriers* (leading to catastrophic floods), *air traffic control* (leading to air disasters), *large-scale production/processing and/or storage of (petro)chemical substances* (leading to an "ecological disaster"), and *heads of State* (leading to their assassination). Their similarities explain the label of this category: *comparable* to kinetic attacks, *directly* leading to *physical damage*. Moreover, some of these targets are even designated "objects containing dangerous forces" and thus explicitly protected by international law.[17]

Comparing the expert judgements with regard to when this category triggers the Netherlands' right of self-defense, led to the suggestion that cyber-attacks launched against Category I targets would have to create one or more of the following effects (from most important to less important): (a) a physical damage of 1 or more persons dead, (b) a societal damage of at least 100,000 people with serious societal survivability problems, and/or (c) an economic damage of at least 5,000,000,000 euros (with the remark that using only economic damage as a qualifier is difficult, due to the reluctant official position of the Netherlands' government).[18]

After conducting the interviews, it also became clear that disruption, degradation or destruction of *essential medical services*—specifically mentioned by the UK as a potential armed attack—is another example of this first category. Theoretically, it was excluded, because it is not (yet) a Netherlands' vital process, but since attacking *essential medical services* leads *directly* to *physical damage*, 1 or more persons dead would suffice to qualify as an armed attack.

5.2. Contributing criteria for cyber-attacks comparable to kinetic attacks, indirectly leading to physical damage

Identification of this second category is based on the similarities between the scenarios that comprised disruption, degradation or destruction of *production, distribution and transport of electricity, gas and oil* (leading to the unavailability of electricity or other forms of energy), *clean water supply* (leading to the unavailability of fresh water), and *communications networks* (necessary for "policing"). Also, in this case, their similarities explain the label of this category: *comparable* to kinetic attacks, *indirectly* leading to *physical damage*. Compared to the previous category, their nature is less self-evident, implying that the threshold for qualifying as an armed attack is higher, as well as the level of substantiation necessary for demonstrating the (indirect) harmful effects.

Comparing the expert judgements with regard to when this category triggers the Netherlands' right of self-defense, led to the suggestion that cyber-attacks launched against Category II targets would have to create one or more of the follow-on effects (from most important to less important): (a) a physical damage of more than 1000 people dead, seriously injured or chronically sick, (b) a societal damage of 100,000–1,000,000 people with serious societal survivability problems, and/or (c) an economic damage of 5,000,000,000–50,000,000,000 euros (with the remark that using only economic damage as a qualifier is difficult, due to the reluctant official position of the Netherlands' government).[19]

5.3. Contributing criteria for cyber-attacks not comparable to kinetic attacks, leading to societal disruption

Identification of this third category is mainly based on the scenario that comprised disruption, degradation or destruction of *financial systems* (including government processes for "taxation"), and possibly complemented by—although considered less likely to reach the suggested threshold—*internet itself* (disabling the digital infrastructure or services necessary for the functioning of society). Despite the caveat regarding cyber-attacks conducted against *internet itself*, this category consists of cyber-attacks that are *not comparable* to kinetic attacks and (probably) "only" cause *societal* and *economic* damage, making their nature the least self-evident and their effects the most non-kinetic compared to the previous two categories. This implies that the necessary level of substantiation is the highest of all categories, as well as the threshold for qualifying as an armed attack.

The purest criterion—according to the leading Dutch cyber experts—for this category to trigger the Netherlands' right of self-defense, is achieving "societal disruption." Unfortunately, like "armed attack," "societal disruption"—combined with "serious societal survivability problems" for a number of people—lacks a clear definition. Although the Netherlands Scientific Council for Government Policy (WRR) states that "digital societal disruption" occurs "when normal life is seriously and adversely affected" (The Netherlands Scientific Council for Government Policy 2019, 7), it also recognizes the absence of a tangible threshold and how difficult it is to overcome this lacuna (Wetenschappelijk Raad voor het Regeringsbeleid 2019, 25). The WRR hints toward "key societal systems and institutions being visibly impacted," and "citizens losing confidence in the institutions of government, the market economy and the society in which they live" (The Netherlands Scientific Council for Government Policy 2019, 6–7), but further clarification would need additional research.

Nevertheless, the leading Dutch cyber experts—particularly the two legal experts—generally accepted the upper limits of the suggested bandwidths for societal and economic damage as a guideline for the (absolute) minimum threshold.[20] This would imply the suggestion that cyber-attacks launched against Category III targets trigger the Netherlands' right of self-defense if it leads to one or more of the following effects: (a) a societal damage of at least 1,000,000 people with serious societal survivability problems, and/or (b) an economic damage of at least 50,000,000,000 euros (with the remark that using only economic damage as a qualifier is difficult, due to the reluctant official position of the Netherlands' government).[21]

To conclude this section, Figure 1 provides a schematic overview of the synthesis resulting in contributing criteria that could trigger the Netherlands' right of self-defense for three cyber armed attack-categories.

6. Concluding reflections

By interpreting the legal guidance for armed attacks in cyberspace, and cross-fertilizing it with international and interdisciplinary policy documents, including the opinion of leading Dutch cyber experts, this paper has offered further granularity in the discourse on *scale* and *effect* regarding cyber-attacks that might qualify as an armed attack in the meaning of Article 51 of the UN Charter, triggering the right of self-defense in international relations. This granularity could enable us to take away some of the legal "uncertainty" (Schmitt 2017, 346, Rule 72, para 20) articulated in the Tallinn Manual 2.0.

The result of the conducted synthesis is a policy framework with a categorization that will provide more clarity for (a) the author of a cyber-attack with regard to when the armed attack-threshold is reached in cyberspace and (b) when a victim State can respond in self-defense to cyber-attacks with a grave impact. However, three aspects need to be addressed to ensure the proper interpretation and implementation of the suggested policy framework.

First, as already mentioned, it must be clear that the suggested levels for each category originate from the (minimum) expected effects in case of disruption,

Categories of armed attack in cyberspace	Practical examples (of disrupted, degraded or destructed 'core security assets')	Characteristics	Contributing criteria that could trigger the NL right of self-defense *(from most important to less important with the remark that using only economic damage as a qualifier is difficult, due to the reluctant official position of the Netherlands' government)*
I	*Production, storage and processing of nuclear material* (leading to a nuclear disaster)	- comparable to kinetic attacks - *directly* leading to physical damage	(a) a *direct* physical damage of 1 or more persons dead (b) a societal damage of at least 100,000 people with serious societal survivability problems (c) an economic damage of at least 5,000,000,000 euros
	Water barriers (leading to catastrophic floods)		
	Large-scale production/processing and/or storage of (petro)chemical substances (leading to an 'ecological disaster')		
	Air traffic control (leading to air disasters)		
	Heads of State (leading to their assassination)		
	Essential medical services (leading to dying patients)		
II	*Production, distribution and transport of electricity, gas and oil* (leading to the unavailability of electricity or other forms of energy)	- comparable to kinetic attacks - *indirectly* leading to physical damage	(a) an *indirect* physical damage of more than 1,000 people dead, seriously injured or chronically sick (b) a societal damage of 100,000 – 1,000,000 people with serious societal survivability problems (c) an economic damage of 5,000,000,000 – 50,000,000,000 euros
	Clean water supply (leading to the unavailability of fresh water)		
	Communications networks (necessary for 'policing')		
III	*Financial systems* (including government processes for 'taxation')	- not comparable to kinetic attacks - leading to 'societal disruption'	'Societal disruption', the *purest criterion* for this category, could be achieved with: (a) a societal damage of at least 1,000,000 people (as an absolute minimum) with serious societal survivability problems (b) an economic damage of at least 50,000,000,000 euros (as an absolute minimum)
	Internet itself (disabling the digital infrastructure or services necessary for the functioning of society)		

Figure 1. Policy framework regarding when cyber-attacks qualify as an armed attack, triggering the Netherlands' right of self-defense.

degradation or destruction of Netherlands' vital processes. Although the original impact levels are official policy from the Ministry of Justice and Security,[22] they were not defined to categorize cyber-attacks or determine if they qualify as an armed attack. Nevertheless, while existing sources in international law provide no tangible guidance for judging whether the *scale* and *effect* of cyber operations can be appraised as relatively large and substantial, the applied form of cross-fertilization offers a potential solution for this problem.

Secondly, and this has also been mentioned already, the suggested categorization is currently quantified for the Netherlands' situation. However, it could perhaps be widened by applying relative criteria: using percentages of the population size or of the gross national/domestic product as contributing criteria could possibly make the thresholds suitable for other States as well.

Thirdly, and most importantly, by recognizing a category of armed attack in cyberspace that is *not comparable* to kinetic attacks, leading to *societal disruption* (Category III), the suggested policy framework positions itself in a situation similar to the 1945 Brazilian proposal on the use of force interpretation in the UN Charter, arguing that apart from a prohibition on the threat and use of force, a similar transboundary prohibition should apply to "mesure d'ordre économique."[23] Therefore, ignited by the emergence of cyberspace, a discourse should commence on what the width and depth of the use of force and subsequently an armed attack is in cyberspace, and whether *societal disruption*—caused by serious societal survivability problems for a (relatively large) number of people and/or (substantial) economic damage—could indeed be a valid criterion for armed attack-qualification, as argued in this paper. And if so, then

perhaps the current non-eligibility of "cyber espionage" and "manipulation of the information environment" for armed attack qualification—presumed earlier in this paper—would have to be reconsidered, assuming that both types of cyber-attacks could indeed be grave enough to cause *societal disruption*.

Notes

1. Article 51 UN Charter (San Francisco, 1945).
2. See e.g. Switzerland's position paper on the application of international law in cyberspace—Annex to the UN GGE 2019/2021, 4. The Swiss legal opinion underlines that there are no binding quantitative or qualitative guidelines as to when the threshold of an armed attack in terms of scale and effect has been reached.
3. See the United Nations Office of Disarmament Affairs on Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security. https://www.un.org/disarmament/group-of-governmental-experts/.
4. Caveat: the scenario regarding cyber-attacks conducted against *military capacity* (making it impossible to deploy the armed forces) was theoretically identified as a potential armed attack during the desk research but excluded from the field research due to the specific focus on civilian (i.e. non-military) targets.
5. That is, intervention on invitation, authorisation based on Chapter VII of the UN Charter, self-defense. See for example, Lowe (2007, 103).
6. Case Concerning Military and Paramilitary Activities in and against Nicaragua, ICJ Reports (1986), para 190, 100. A peremptory norm of international law (jus cogens) is a norm from which no derogation is permitted and which can be modified only by a norm of international law having the same character.
7. The Brazilian proposal to include "mesure d'ordre économique."
8. Although most States recognize the gap between both articles, one does not: the US. Its position is that any "use of force" triggers the right of self-defense, even though the rest of the world focusses on Article 51 of the UN Charter which talks about "armed attack" (University of Virginia School of Law 2017; Schmitt 2013a, 689; Schmitt 2013b, 332–333, Rule 69, para. 7).
9. Regarding the sources of law, according to Article 38(1) of the Statute of the ICJ, customary law takes precedence over the opinions of leading academics. However, the customary international law is far from solidified in this matter: state practice is lacking and the legal opinions of only a few States are available. Since the opinions of leading academics were developed first and potentially influenced the positions of States, these will be dealt with first.
10. Although this guidance was articulated for determining if cyber operations violate the prohibition of the use of force, in this paper, it is also considered important in relation to an armed attack, since armed attack is depicted to have a higher threshold than the use of force-standard (Schmitt 2015, 1115).
11. While numerous states have provided legal opinion on the application of international law to cyberspace, most express their position in generic terms. See Schmitt (2019). The position of the US will not be addressed since it holds the view that the threshold for the use of force and armed attack are identical, see Schmitt (2020), Schmitt (2013a, 689), and Schmitt (2017, 332–333, Rule 69, para. 7).
12. Cyber Espionage is the non-consensual collection of confidential information. Whilst cyber espionage can be executed in peacetime or during armed conflict, it does not reach the threshold of the use of force. See also Buchan and Navarrete (2021, 232–235).
13. Whyte and Mazanec identify 4 types of attacks. Supporting kinetic attacks is the fourth category which is excluded from this analysis. See also National Coordinator for Security and Counterterrorism (2019).

14. Compare: the attacks on 9/11. See Hosang and Ducheine.
15. The (validated) interview reports and the data analysis matrix—on which this section is based—are not included but can be provided upon request.
16. *Interview report A2: senior legal expert Ministry of Defense*, 93, Scenario 2, para. 1.
17. *Interview report A2: senior legal expert Ministry of Defense*, 92, Scenario 1, para. 2.
18. *Data analysis matrix*, 128.
19. Ibid.
20. *Interview report A1: senior legal expert Ministry of Foreign Affairs*, 88, Scenario 9, para. 1; and *Interview report A2: senior legal expert Ministry of Defense*, 98, Scenario 9, para. 1.
21. *Data analysis matrix*, 129.
22. Appendix C, *Netherlands' 2-tier categorization of vital processes*, 89.
23. See note 20 supra (above).
24. See the caveat in note 4.

Disclosure statement

No potential conflict of interest was reported by the author(s).

References

AIV/CAVV. 2011. *Cyber Warfare – No 77, AIV/No 22, CAVV December 2011*. The Hague: Advisory Council on International Affairs (AIV)/Advisory Committee on Issues of Public International Law (CAVV).

Amadeo, Kimberly. 2020. "How the 9/11 Attacks Affect the Economy Today." *The Balance*, February 22. https://www.thebalance.com/how-the-9-11-attacks-still-affect-the-economy-today-3305536

Amer, Karim, and Jehane Noujaim, dir. 2019. "The Great Hack." *A Netflix Original Documentary*, Video.

Attorney General's Office. 2018. *Speech: Cyber and International Law in the 21st Century*. May 23. https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century

Bijleveld, Ank. 2018. "Keynote by HE Ms. Ank Bijleveld MA, Minister of Defence." *Militair Rechtelijk Tijdschrift: Cyber Special*, 45–47.

Boddens Hosang, J. F. R., and P. A. L. Ducheine. 2020. "Implementing Article 42.7 of the Treaty on European Union: Legal Foundations for Mutual Defence in the Face of Modern Threats." *Amsterdam Law School Research Papers*, no. 2020-71. https://ssrn.com/abstract=3748392

Boothby, William H., Wolff Heintschel von Heinegg, James Bret Michael, Michael N. Schmitt, and Thomas C. Wingfield. 2012. "When Is a Cyberattack a Use of Force or an Armed Attack?" *Computer Magazine* 45 (8): 82–84. doi:10.1109/MC.2012.282.

Broeders, Dennis. 2021. "The (Im) Possibilities of Addressing Election Interference and the Public Core of the Internet in the UN GGE and OEWG : A Mid-Process Assessment." *Journal of Cyber Policy* 6 (3): 277–297. doi:10.1080/23738871.2021.1916976.

Buchan, Russell, and Inaki Navarrete. 2021. "Cyber Espionage and International Law." In *Research Handbook on International Law and Cyberspace*, 2nd ed., edited by Nicholas Tsagourias and Russell Buchan, 231–252. Cheltenham: Edward Elgar Publishing.

Dinnis, Heather Harrison. 2012. *Cyber Warfare and the Laws of War*. New York, NY: Cambridge University Press.

Dinstein, Yoram. 2013. "Cyber War and International Law: Concluding Remarks at the 2012 Naval War College International Law Conference." *International Law Studies* 89: 276–287.

Ducheine, P. A. L., and B. M. J. Pijpers. 2021. "The Notion of Cyber Operations." In *Research Handbook on International Law and Cyberspace*, 2nd ed., edited by Nicholas Tsagourias and Russell Buchan, 271–295. Cheltenham: Edward Elgar Publishing.
Gill, Terry D. 2015. "Legal Basis of the Right of Self-Defence under the UN Charter and under Customary International Law." In *The Handbook of the International Law of Military Operations*, edited by Terry D. Gill and Dieter Fleck, 213–224. Oxford: Oxford University Press.
Gill, Terry D. 2015. "Military Intervention with the Consent or at the Invitation of a Government." In *The Handbook of the International Law of Military Operations*, edited by Terry D. Gill and Dieter Fleck, 252–255. Oxford: Oxford University Press.
Gill, Terry D., and Kinga Tibori-Szabó. 2019. "Twelve Key Questions on Self-Defense against Non-State Actors – and Some Answers." *International Law Studies* 95: 479–482.
Gill, Terry D., and Paul A. L. Ducheine. 2013. "Anticipatory Self-Defense in the Cyber Context." *International Law Studies* 89: 438–471.
Hakim, Danny, and Matthew Rosenberg. 2018. "Data Firm Tied to Trump Campaign Talked Business with Russians." *The New York Times*, March 17. https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-russia.html
ICJ. 1986. *Case Concerning Military and Paramilitary Activities in and against Nicaragua (Judgment) (Nicaragua v. United States)*. ICJ Reports.
ICJ. 1996. *Case concerning the Legality of the Threat or Use of Nuclear Weapons* (Advisory Opinion). ICJ Reports.
ICJ. 2003. *Case Concerning Oil Platforms (Iran v. United States) (Judgment)*. ICJ Reports.
ICJ. 2005. *Case Concerning Armed Activities on the Territory of the Congo (DRC v. Uganda) (Judgment)*. ICJ Reports.
Kerschischnig, Georg. 2012. *Cyberthreats and International Law*. The Hague: Eleven International Publishing.
Lowe, Vaughan. 2007. *International Law. Clarendon Law Series*. Oxford: OUP Oxford.
Mačák, Kubo. 2017. "From Cyber Norms to Cyber Rules: Re-Engaging States as Law-Makers." *Leiden Journal of International Law* 30 (4): 877–899. doi:10.1017/S0922156517000358.
Maurer, Tim. 2018. *Cyber Mercenaries: The State, Hackers and Power*. Cambridge: Cambridge University Press.
Ministère des Armées. 2019. "International Law Applied To Operations In Cyberspace." *République Française*, September 9. https://www.defense.gouv.fr/content/download/567648/9770527/file/international+law+applied+to+operations+in+cyberspace.pdf
Minister of Foreign Affairs. 2019. "Letter to the Parliament on the International Legal Order in Cyberspace." *Government of the Netherlands*, July 5. https://www.government.nl/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace
Nationaal Coördinator Terrorismebestrijding en Veiligheid. 2020. "Overzicht Vitale Processen." *Ministerie van Justitie en Veiligheid*. Accessed April 30, 2020. https://www.nctv.nl/onderwerpen/vitale-infrastructuur/overzicht-vitale-processen.
National Coordinator for Security and Counterterrorism. 2019. "Cyber Security Assessment Netherlands 2019." *Ministry of Justice and Security*, June. https://english.ncsc.nl/topics/cyber-security-assessment-netherlands/documents/publications/2019/09/13/cyber-secrurity-assessment-netherlands-2019
National Cyber Security Centre. 2018. "New Cyber Attack Categorisation System to Improve UK Response to Incidents." *The Government of the United Kingdom*, April 11. https://www.ncsc.gov.uk/news/new-cyber-attack-categorisation-system-improve-uk-response-incidents
Parliamentary Papers II 2019–2020, 33 694, nr 47. 2019. "Internationale Veiligheidsstrategie: Brief van de minister van Buitenlandse Zaken." July 5.
Parliamentary Papers II 2019–2020, 33 694, nr 57. 2019. "Internationale Veiligheidsstrategie: Brief van de minister van Buitenlandse Zaken." April 17.
Pijpers, B. M. J., and P. A. L. Ducheine. 2020. "Influence Operations in Cyberspace – How They Really Work." *Amsterdam Law School Research Papers* 2020–61.

Pijpers, B. M. J. 2022. "Influence Operations in Cyberspace: On the Applicability of Public International Law during Influencing Operations in a Situation below the Threshold of the Use of Force." PhD thesis, University of Amsterdam.
Randelzhofer, A. 1994. "Article 51." In *The Charter of the UN: A Commentary*, edited by Bruno Simma, 661–678. München: C.H. Beck Verlag.
Roscini, Marco. 2014. *Cyber Operations and the Use of Force in International Law*. Oxford: Oxford University Press.
Ruys, Tom. 2010. *"Armed Attack" and Article 51 of the UN Charter: Evolutions in Customary Law and Practice*. Cambridge: Cambridge University Press.
Schmitt, Michael N. 2012. "'Attack' as a Term of Art in International Law: The Cyber Operations Context." 4th International Conference on Cyber Conflict, no. 2010.
Schmitt, Michael N. 2013a. "Cyber Activities and the Law of Countermeasures." In *Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy*, edited by Katharina Ziolkowski, 659–690. Tallinn: NATO CCD COE Publication.
Schmitt, Michael N. 2013b. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press.
Schmitt, Michael N. 2017. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press.
Schmitt, Michael N. 2020. "Taming the Lawless Void: Tracking the Evolution of International Law." *Texas National Security Review* 3 (3): 32–47.
Schmitt, Michael N. 2019a. "France's Major Statement on International Law and Cyber: An Assessment." *Just Security*, no. 2.
Schmitt, Michael N. 2019b. *The Netherlands Releases a Tour de Force on International Law in Cyberspace: Analysis*, October 14. https://www.justsecurity.org/66562/the-netherlands-releases-a-tour-de-force-on-international-law-in-cyberspace-analysis/
Schmitt, Michael N. 2015. "The Use of Cyber Force and International Law." In *The Oxford Handbook of the Use of Force in International Law*. Oxford University Press.
Schmitt, Michael N. 2018. "'Virtual' Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law." *Chicago Journal of International Law* 19 (1): 30–67. https://chicagounbound.uchicago.edu/cjil/vol19/iss1/2
Secrétariat Général de la Défense et de la Sécurité Nationale. 2018. "Revue stratégique de cyberdéfense." *République Française*, February 12. http://www.sgdsn.gouv.fr/uploads/2018/02/20180206-np-revue-cyber-public-v3.3-publication.pdf
Sits, Kristi. 2019. *President of the Republic at the Opening of CyCon 2019*, May 29. https://president.ee/en/official-duties/speeches/15241-president-of-the-republic-at-the-opening-of-cycon-2019/
The Netherlands Scientific Council for Government Policy. 2019. *Preparing for Digital Disruption: Summary of WRR Report 101*. The Hague: WRR.
Tolppa, Maria. 2020. "Overview of the UN OEWG Developments: Continuation of Discussions on How International Law Applies in Cyberspace." *NATO CCD COE*, March 23. https://ccdcoe.org/incyder-articles/?year=2020
UN. 1945a. *Statute of the ICJ*. San Francisco, CA: UN.
UN. 1974. *UN General Assembly Resolution 3314 (XXIX): Definition of Aggression*, December 14.
UN General Assembly. 2021. "Official Compendium of Voluntary National Contributions on the Subject of How International Law Applies to the Use of Information and Communications Technologies – A/76/136." July.
UN GGE 2015 Report. 2015. "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security – A/70/174." Vol. 12404.
UNIO (UN Information Organization) 1945. "United Nations Conference on International Organization (UNCIO) – Volume VI."

University of Virginia School of Law. 2017. "Cyber and the Law of Armed Conflict." *YouTube*, November 21, Video. Accessed March 8, 2020. https://www.youtube.com/watch?v=EuGVTN5UHLc

Valeriano, Brandon, and Ryan C. Maness. 2015. *Cyber War versus Cyber Realities: cyber Conflict in the International System*. New York, NY: Oxford University Press.

Whyte, Christopher, and Brian Mazanec. 2019. *Understanding Cyber Warfare: Politics, Policy and Strategy*. London; New York, NY: Routledge Taylor & Francis Group.

Wetenschappelijk Raad voor het Regeringsbeleid. 2019. *Voorbereiden Op Digitale Ontwrichting: WRR-Rapport 101*. Den Haag: WRR.

Appendix A

Cyber-attack scenarios for which The Netherlands' armed attack-threshold could lie somewhere in the defined bandwidths

Appendix A presents a visualization of the theoretical analysis resulting in an overview of the cyber-attack scenarios for which the Netherlands' armed attack-threshold could lie somewhere within the defined bandwidths, and additionally includes the heads of State criterium of the IGE. This overview, based on desk research, was used as a baseline to conduct structured interviews to collect verbal statements from leading cyber experts (as if they were advising their minister) from the Netherlands' ministries of (a) Foreign Affairs, (b) Defense, and (c) Justice and Security regarding when these theoretically identified potential armed attacks in cyberspace would actually reach the armed attack-threshold in practice and, therewith, trigger the Netherlands' right of self-defense.

No 'use of force'	Cyber-attacks eligible for qualification as an armed attack in cyberspace (if sufficiently grave)	Corresponding Netherlands' Category A and B vital processes (i.e. 'core security assets')	Bandwidths based on the (minimum) expected effects in case of 'disruption, degradation or destruction' of Netherlands' Category A and B vital processes (i.e. 'core security assets')
Cyber espionage			
Manipulation of the information environment			
	Disruption, degradation or destruction of 'core security assets'		
	Production, storage and processing of nuclear material (leading to a nuclear disaster)	Cat A (and British political support)	**Suggestion in this paper based on desk research:** The threshold for these cyber-attack scenarios to be grave enough in *scale* and *effect* to qualify as an armed attack, and trigger the Netherlands' right of self-defence, could lie somewhere between the 'expected damage levels' – defined by the Ministry of Justice and Security – for Netherlands' Category A and Category B vital processes (see Appendix D). This implies that disruption, degradation or destruction of these 'core security assets' should cause a *physical*, *societal* or *economic* damage of: *** 1,000 – 10,000 people dead, seriously injured or chronically sick;** *** 100,000 – 1,000,000 people with serious societal survivability problems;** *** 5,000,000,000 – 50,000,000,000 euros.**
	Production, distribution and transport of electricity, gas and oil (leading to the unavailability of electricity or other forms of energy)	Cat A	
	Water barriers (leading to catastrophic floods)	Cat A	
	Clean water supply (leading to the unavailability of fresh water)	Cat A	
	Internet itself (disabling the digital infrastructure or services necessary for the functioning of society)	Cat B (and Estonian political support)	
	Air traffic control (leading to air disasters)	Cat B (and British political support)	
	Large-scale production/processing and/or storage of (petro)chemical substances (leading to an 'ecological disaster')	Cat B (and French political support)	
	Financial systems (including government processes for 'taxation')	Cat B (and Dutch political support: keynote speech MoD)	
	Communications networks (necessary for 'policing')	Cat B (and Dutch political support: keynote speech MoD)	
	Heads of State (leading to their assassination)	(No Dutch 'vital process', but unanimously supported by the IGE)	
	Military capacity (making it impossible to deploy the armed forces)	Cat B (and Dutch political support: AIV/CAVV Report), but excluded from the field research due to the specific focus on non-military targets	

Cyber-attack scenarios for which the Netherlands' armed attack-threshold could lie somewhere in the defined bandwidths[2]

Cyber-attack scenarios for which the Netherlands' armed attack-threshold could lie somewhere in the defined bandwidths.[24]

Appendix B

French 5-tier categorization of the gravity or severity of cyber-attacks (UN General Assembly 2021; Secrétariat Général de la Défense et de la Sécurité Nationale 2018, 80)

Echelle de gravité	*Equivalence avec l'échelle CISS USA*	Caractérisation de l'impact	Caractérisation comme agression armée au sens de l'article 51 de la Charte des Nations-Unies
Niveau 5 - *Situation d'urgence extrême*	*Level 5 Emergency (Black)*	Impact extrême	Probablement possible : à examiner au cas par cas.
Niveau 4 - *Crise majeure*	*Level 4 Severe (Red)*	Impact majeur	Probablement impossible : les actions correspondant à ces niveaux pourraient néanmoins constituer d'autres faits internationaux illicites (intervention, violation de la souveraineté, usage de la force, etc.).
Niveau 3 - *Crise*	*Level 3 High (Orange)*	Impact fort et étendu	
Niveau 2 - *Incident grave*	*Level 2 Medium (Yellow)*	Impact fort et circonscrit	
Niveau 1B - *Incident*	*Level 1 Low (Green)*	Impact significatif et circonscrit	
Niveau 1A - *Evénement significatif*		Impact faible	
Niveau 0 - *Evénement*	*Level 0 Baseline (White)*	Impact négligeable	

Schéma national de classement des attaques informatiques

Appendix C

British 5-tier categorization of the gravity or severity of cyber-attacks (National Cyber Security Centre 2018)

	Category definition	Who responds?	What do they do?
Category 1 National cyber emergency	A cyber attack which causes sustained disruption of UK essential services or affects UK national security, leading to severe economic or social consequences or to loss of life.	Immediate, rapid and coordinated cross-government response. Strategic leadership from Ministers / Cabinet Office (COBR), tactical cross-government coordination by NCSC, working closely with Law Enforcement	Coordinated on-site presence for evidence gathering, forensic acquisition and support. Collocation of NCSC, Law Enforcement, Lead Government Departments and others where possible for enhanced response.
Category 2 Highly significant incident	A cyber attack which has a serious impact on central government, UK essential services, a large proportion of the UK population, or the UK economy.	Response typically led by NCSC (escalated to COBR if necessary), working closely with Law Enforcement (typically NCA) as required. Cross-government response coordinated by NCSC.	NCSC will often provide on-site response, investigation and analysis, aligned with Law Enforcement criminal investigation activities.
Category 3 Significant incident	A cyber attack which has a serious impact on a large organisation or on wider / local government, or which poses a considerable risk to central government or UK essential services.	Response typically led by NCSC, working with Law Enforcement (typically NCA) as required.	NCSC will provide remote support and analysis, standard guidance; on-site NCSC or NCA support may be provided.
Category 4 Substantial incident	A cyber attack which has a serious impact on a medium-sized organisation, or which poses a considerable risk to a large organisation or wider / local government.	Response led either by NCSC or by Law Enforcement (NCA or ROCU), dependent on the incident.	NCSC or Law Enforcement will provide remote support and standard guidance, or on-site support by exception.
Category 5 Moderate incident	A cyber attack on a small organisation, or which poses a considerable risk to a medium-sized organisation, or preliminary indications of cyber activity against a large organisation or the government.	Response led by Law Enforcement (likely ROCU or local Police Force), with NCA input as required.	Law Enforcement will provide remote support and standard guidance, with on-site response by exception.

Appendix D

Netherlands' 2-tier categorization of vital processes (Nationaal Coördinator Terrorismebestrijding en Veiligheid 2020)

Vitale processen	Categorie	Sector	Ministerie
Landelijk transport en distributie elektriciteit	A	Energie	EZK
Regionale distributie elektriciteit	B		
Gasproductie, landelijk transport en distributie gas	A		
Regionale distributie gas	B		
Olievoorziening	A		
Internet en datadiensten	B	ICT/Telecom	EZK
Internettoegang en dataverkeer	B		
Spraakdienst en SMS*	B		
Plaats- en tijdsbepaling middels GNSS	B		IenW
Drinkwatervoorziening	A	Drinkwater	IenW
Keren en beheren waterkwantiteit	A	Water	IenW
Vlucht- en vliegtuigafhandeling	B	Transport	IenW
Scheepvaartafwikkeling	B		
Vervoer van personen en goederen over (hoofd)spoorweginfrastructuur	B	Transport	IenW
Vervoer over (hoofd)wegennet	B	Transport	IenW
Grootschalige productie/verwerking en/of opslag (petro)chemische stoffen	B	Chemie	IenW
Opslag, productie en verwerking nucleair materiaal	A	Nucleair	IenW
Toonbankbetalingsverkeer	B	Financieel	FIN
Massaal giraal betalingsverkeer	B		
Hoogwaardig betalingsverkeer tussen banken	B		
Effectenverkeer	B		
Communicatie met en tussen hulpdiensten middels 112 en C2000	B	OOV	JenV
Inzet politie	B		

Basisregistraties personen en organisaties	B	Digitale overheids-processen	BZK
Interconnectiviteit (transactie-infrastructuur voor informatie uit basisregistraties)	B		
Elektronisch berichtenverkeer en informatieverschaffing aan burgers	B		
Identificatie en authenticatie van burgers en bedrijven	B		
Inzet defensie	B	Defensie	DEF

* voor alle ICT/Telecomprocessen geldt dat deze zowel via vaste als mobiele aansluitingen en infrastructuur worden verzorgd, met uitzondering van SMS, hier geldt alleen dat deze via mobiele aansluitingen en infrastructuur worden verzorgd.

Categorie A

In deze categorie staat de infrastructuur die bij verstoring, aantasting of uitval de ondergrenzen van minstens één van de drie impactcriteria (economisch, fysiek of sociaal maatschappelijk) voor categorie A raakt en daarnaast ook voldoet aan het criterium van cascade gevolgen:

- Economische gevolgen: > ca. 50 miljard euro schade of ca. 5,0 % daling reëel inkomen
- Fysieke gevolgen: meer dan 10.000 personen dood, ernstig gewond of chronisch ziek
- Sociaal maatschappelijke gevolgen: meer dan 1 miljoen personen ondervinden emotionele problemen of ernstig maatschappelijke overlevingsproblemen
- Cascade gevolgen: Uitval heeft als gevolg dat minimaal twee andere sectoren uitvallen.

Categorie B

In deze categorie staat de infrastructuur die bij verstoring, aantasting of uitval de ondergrenzen van minstens één van de drie impactcriteria voor categorie B raakt:

- Economische gevolgen: > ca. 5 miljard euro schade of ca. 1,0 % daling reëel inkomen
- Fysieke gevolgen: meer dan 1.000 personen dood, ernstig gewond of chronisch ziek
- Sociaal maatschappelijke gevolgen: meer dan 100.000 personen ondervinden emotionele problemen of ernstig maatschappelijke overlevingsproblemen