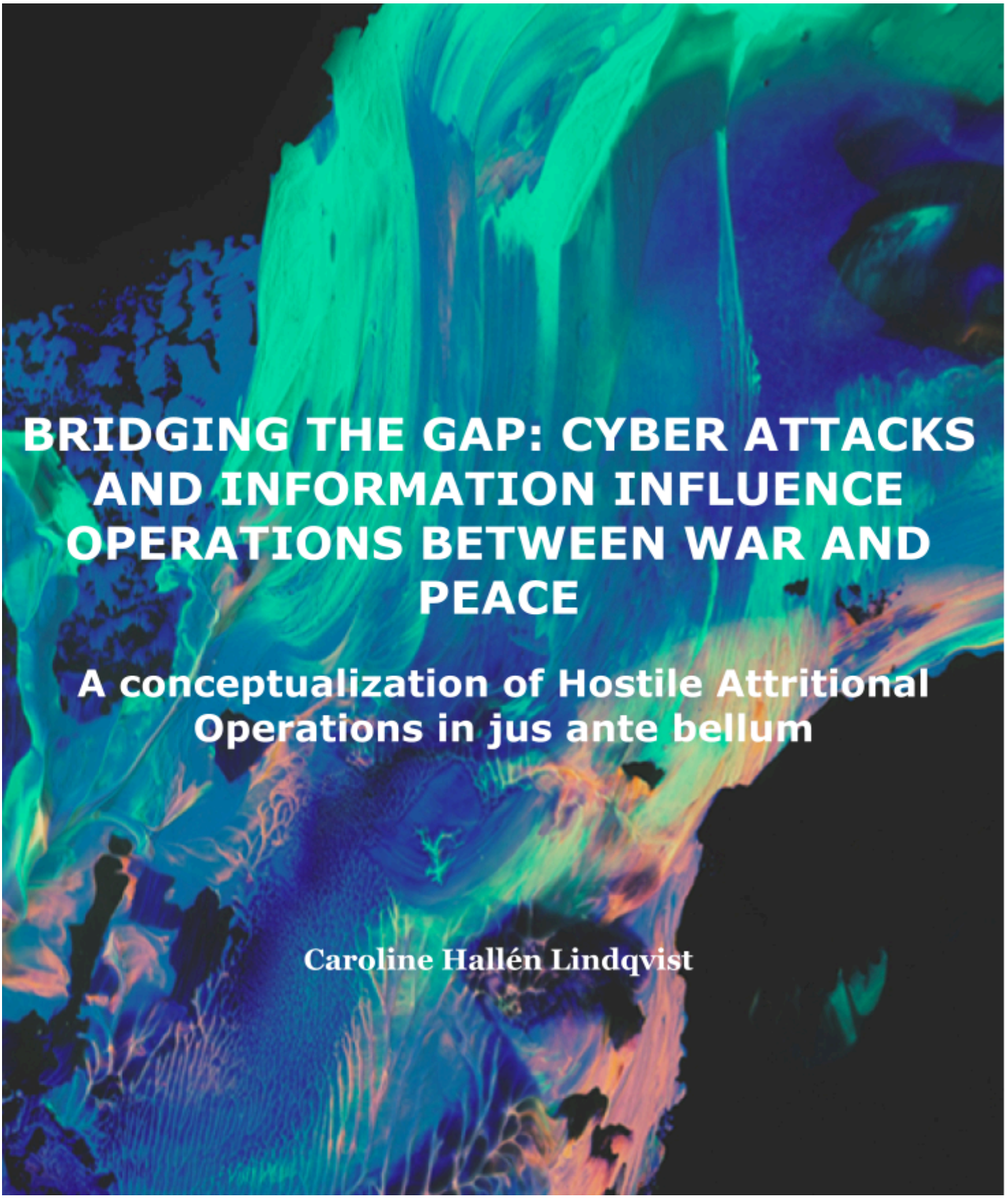
UMEÅ UNIVERSITET



BRIDGING THE GAP: CYBER ATTACKS AND INFORMATION INFLUENCE OPERATIONS BETWEEN WAR AND PEACE

A conceptualization of Hostile Attritional Operations in jus ante bellum

Caroline Hallén Lindqvist

Fall semester 2024
Master thesis in public international law, 30 credits
Master of Laws, 270 credits
Supervisor: Emil Wistrand Johansson

Abstract

Problems arising from hybrid warfare have been increasing in later days, to a large extent enabled by developments in technology. This type of conduct can take place both before and during warfare, but is sometimes of the character that mimics preparations for war, or what one could call attritional, *pre-war* conduct. This thesis has primarily been aimed at establishing Hostile Attritional Operations (HAO:s)—here thought to consist of cyber attacks and information influence operations-—as a concept of *jus ante bellum*, a legal area of public international law that has not yet been developed to any larger extent outside academia. To accomplish this, first, the central concept of HAO:s has been outlined, before continuing on to examine its applicability to the legal frameworks of peacetime and during armed conflict, respectively. This is exceedingly done in the pursuit of determining whether there is a considerable "gap" or "gray area" between peacetime regulations and those of warfare, which current frameworks of public international law are unable to deal with in an adequate way. Here, some aspects of the LOAC handling of HAO:s are looked to as a possible template for the substantial modeling of HAO:s in jus ante bellum.

In the thesis, the conclusion is made that the respective frameworks—partly due to the difficulties of attributing a conduct to a specific State, but also because of the fragmentation of international law and the strict division between the two—are lacking in some aspects, at least in relation to the countering of pre-war conduct which is prima facie non-violent in nature. Besides the sketching out of a foundation to the handling of HAO:s in jus ante bellum, the ambition is to provide the reader with insights on the challenges of pre-war conduct that consists of non-violent hybrid warfare, as well as illuminating the dangers of leaving jus ante bellum unregulated. Another aspiration is to leave suggestions on further research, where the concept of HAO:s can be used to develop concrete regulations in jus ante bellum. This can include viewing artificial intelligence (AI) as a form of HAO, or how HAO:s can be used to give more steadfast guidance for e.g. NATO member States on how to operate in jus ante bellum.

Key words: Public International Law; Law of Armed Conflict; Jus Ante Bellum; Hostile Attritional Operations; Hybrid Warfare; Cyber Attacks; Information Influence Operations; Peacetime countermeasures.

Acknowledgements

First and foremost, I would like to thank my friends and family for all the ways in which they have helped me achieve the long-held dream of graduating from juristprogrammet at Umeå University. Mom, dad, Peter and Nina have all been the most supportive family members, especially in helping me look after my beloved four-legged friend when time was lacking, and I needed it the most. Elin, Erik and Sara, I could not have asked for better friends and more unwavering support, neither now nor during our time at university—even if we went in different paces and ended up in different places. Last but not least, I would like to thank my supervisor Emil for the utmost valuable input and guidance during the writing process of this thesis. Turns out, it takes a village to write a thesis!

Table of contents

Bibliography

International documents
Treaties
Resolutions
Other (UN) documents
Commission reports
Court cases
International Court of Justice (ICJ) cases
Permanent Court of International Justice (PCIJ)
International Criminal Tribunal for the former Yugoslavia (ICTY) cases and reports
Literature
Anthologies
Book chapters
Books
International Red Cross Committee Commentaries
Periodical journals
Internet sources
Consulted reference literature

Abbreviations

ARSIWA	Articles on Responsibility of States for Internationally Wrongful Acts (by the International Law Commissions)
HAO/HAO:s	Hostile Attritional Operation(s)
GA/UNGA	General Assembly (of the United Nations)
IAC	International Armed Conflict
ICESCR	International Covenant on Economic, Social and Cultural Rights
ICISS	International Commission on Intervention and State Sovereignty
ICJ	International Court of Justice
ICCPR	International Covenant on Civil and Political Rights
ICRC	International Committee of the Red Cross
ICT	Information and Communication Technology
ICTY	International Criminal Tribunal of the former Yugoslavia
IHL	International Humanitarian Law
IHRL	International Human Rights Law
ILA	International Law Association
ILC	International Law Commission
NATO	North Atlantic Treaty Organisation
UN Charter	The Charter of the United Nations
VCLT	Vienna Convention on the Law of Treaties (1969)

1 Introduction

> "The first casualty when war comes is truth, and whenever an individual nation seeks to coerce by force of arms another, it always acts, and insists that it acts in self-defense." — Hiram Johnson[1]

> "We live in a world where all wars begin as cyber wars […] it's the combination of hacking and massive, well-coordinated disinformation campaigns." — Jared Cohen[2]

When the President of the Russian Federation announced that Russia was about to initiate its full scale invasion of Ukraine in the early morning hours of the 22th of February 2022, the conflict which had been brewing to-and-fro since the illegal annexation of Crimea in 2014 was now—apparent to most—a clear-cut war. The communication stemming from the Kremlin at the time could be depicted as an attempt to paint the aggression as a self-defense, which had to be carried out in order to protect Russia and the Russian minorities of those breakaway regions of eastern Ukraine, otherwise known as Donetsk and Luhansk (or, in tandem, Donbas).[3] But the attempts to influence the perception of the aggression were not limited to this separate incident; prior to this world-changing event, the Russian regime had put a considerable amount of resources into justifying its acts of aggression on the Ukrainian territory, and this was not the first time that Russia had been accused of engaging in propaganda or, more modernly put, information influence operations.[4] Both the information campaign of 2007 in Estonia and the alleged election interference of U.S. elections in 2016 and 2020 are examples of such hostilities, taking the shape of information operations which are exceedingly aimed at the attrition of the aggrieved State by influencing world views, perceptions and opinions in a way that benefits the State responsible for the conduct.[5]

---

[1] Cited in Locomotive Engineers Journal, February 1929, p. 109.
[2] Cited by Djinis, Elizabeth (2017), "How will cyber warfare change the future? Jared Cohen has some ideas", in Herald-Tribune, available via [https://eu.heraldtribune.com/story/news/local/sarasota/2017/02/20/how-will-cyber-warfare-change-future-jared-cohen-has-some-ideas/22424667007/], accessed 2024-10-24.
[3] See the wording of Vladimir Putin's letter dated 24 February 2022 from the Permanent Representative of the Russian Federation to the United Nations addressed to the Secretary-General (UN Doc. S/2022/154).
[4] See Reisinger and Golts, 2014, p. 1. This is not completely unlike the rhetoric which was used by the then U.S. President George W. Bush, when he initiated the invasion of Iraq in the aftermath of—and supposed response to—the 9/11 terrorist attacks in 2001, see e.g. Bring et al., 2020, p. 183.
[5] Delerue, 2020, p. 495; Johnson, 2020, p. 10; Bring et al., 2020, p. 187; Young (2020), "New Evidence Shows How Russia's Election Interference Has Gotten More Brazen", in Brennan Center for Justice, 2020-03-05, available via [https:// www.brennancenter.org/our-work/analysis-opinion/new-evidence-shows-how-russias-election-interference-has-gotten-more], accessed 2024-10-14. See also examples mentioned in Fogt, 2020, pp. 35 f.f.

While the relativisation of so-called "fake news" is a global worry among individuals,[6] the pre-war measures which have been conducted by States with hostile intentions are not limited to attempts to distort and distribute information. An example of this can be seen in the massive cyber attacks of Ukraine in late December of 2015, which instead targeted Ukrainian infrastructure.[7] In general, both cyber attacks and information influence operations have that in common that they often of the character that they are causing the conflict to take the shape of a more or less one-sided, deniable and non-violent conduct which *prima facie* falls below the threshold of such conduct which constitutes acts of aggression or attacks (or at least being unattributable to a certain State with malign intentions). Instead, the State formally operates in what some would call a "gap" or "gray area" between peacetime and armed conflict, which the State in question uses to gather information of important functions in society, influence and manipulate perceptions, opinions and world-views in politicians as well as in the citizenry, and—long-term—conduct attrition to the State's resilience, as a step on the war to wage regulatory warfare.[8] States with malicious intent are believed to have used this "gray area" between peacetime and armed conflict, what is sometimes called *jus ante bellum* (the events taking place right before war), to conduct both cyber attacks and information influence operations as a step on the way to gain benefits when waging "regular" warfare in the future. In cases when the victim State or international community perceives the possibilities to respond as limited, the perpetrator State can continue its conduct relatively undisturbed.

One question emerging from this is if, and—if so—to what extent are there issues with legally addressing problems pertaining to a situation that takes place between war and peace. In this thesis, Hostile Attritional Operations (HAO:s) is introduced as a jus ante bellum concept. The aim is to examine in what way HAO:s are regulated in international law and what the permissible countermeasures are, in order to determine whether there is a "gap" or "gray area" in jus ante bellum, which current legal frameworks pertinent to that of peacetime and armed conflict, respectively and in tandem, are unable to tackle. By leaning on some aspects of the handlings of HAO:s in armed conflict, a structural and critical approach is applied to the strict division between peacetime regulations and those of armed conflict, as well as the consequences it has for the ability to counter non-violent, pre-war conduct—and exceedingly the possibilities to preserve international peace.

---

[6] World Risk Poll (Gallup), "'Fake news' is the number one worry for internet users worldwide", 2020-06-10, available via [https://wrp.lrfoundation.org.uk/news/fake-news-is-the-number-one-worry-for-internet-users-worldwide], accessed 2024-11-15.

[7] Fogt, 2020, p. 35; ICS Alert, *Cyber-Attack Against Ukrainian Critical Infrastructure*, available via [https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01], accessed 2024-10-15.

[8] Expressen, "Ryska hybridhotet mot Nato: 'Kokande groda'", 2025-01-01, available via [https://www.expressen.se/nyheter/varlden/ryska-hybridhotet-mot-nato-kokande-groda/], accessed 2025-01-01.

1.1 Aims, objectives and research questions

The main aim and purpose of this thesis is to, lex ferenda, conceptualize Hostile Attritional Operations (HAO:s)—i.e. pre-war hybrid warfare in the form of cyber attacks and information influence operations that is taking place in cyberspace, aimed at the attrition of State—as a *jus ante bellum* concept. To achieve this, it is necessary to form an understanding of why both Hostile Attritional Operations (HAO:s) and this kind of development of jus ante bellum is crucial for public international law and its aims of promoting global peace. This, in turn, is done partly by examining the handling of HAO:s according to the frameworks of peacetime and warfare, in order to determine whether the respective frameworks lack in the countering of non-violent, pre-war conduct; mainly in the "gap" or "gray area" between the two frameworks. By drawing on some facets of the handling of HAO:s in the regulation of armed conflict, an attempt is made to sketch out aspects on how the handling of pre-war conduct in jus ante bellum could look like. The following constitutes the research questions of the thesis:

1. What are the legal frameworks applicable to HAO:s in peacetime and armed conflict, respectively?
2. How do these legal frameworks permit the taking of countermeasures against a State responsible for a HAO in the respective frameworks of peacetime and armed conflict? What are the main challenges and uncertainties in the applicable law in this regard?
3. Could a conceptualization of HAO:s in a developing legal framework of *jus ante bellum* contribute to the overcoming of challenges and uncertainties in the legal framework applicable to countermeasures?

1.2 Scope, limitations and some related clarifications

As mentioned in section 1.1 above, the thesis sets aim at conceptualizing HAO:s as a jus ante bellum concept by examining the extent of the assumed "gray area" or "gap" between peacetime and armed conflict, and whether it with regard to the unregulated area of pre-war conduct is motivated to develop principles and (or) regulations in jus ante bellum. In this thesis, focus remains on examining and later comparing the regulations of peacetime as well as that of warfare—i.e. Law of Armed Conflict (LOAC), consisting of International Humanitarian Law (IHL) and International Human Rights Law (IHRL)—and how each one respectively regulate so-called Hostile Attritional Operations (HAO:s), which a hostile State exposes another State, its civilians or its combatants for before or during warfare. These means are used in what can be called a "gray area" kind of warfare, in order to gain military and/or geopolitical advantages.[9] Therefore, the regulations of peacetime in the form of State responsibility, non-intervention, the concepts of sovereignty and bona fide is, as well as those of Law of Armed Conflict (LOAC) (International Humanitarian Law, IHL, and International Human Rights Law, IHRL), are of essence in understanding these phenomenons in international law. With regard to the limited scope of this thesis, attribution questions are only mentioned in the passing.

Furthermore, the thesis for the most part excludes questions pertaining to collective security. Another limitation that is being made is the general exclusion of *jus ad bellum*, i.e. the thesis does not treat the use of force to any greater extent, as HAO:s in both forms (cyber attacks and information influence operations) per definition are such non-violent means that by definition falls outside of the definition of what constitutes a clear violation of the prohibition of use of force in Article 51 of the UN Charter. However, what constitutes a passing of the threshold is necessary to include to a lesser extent, in order to get an understanding of how this relates to HAO:s and why there is a need to develop a legal area where they are regulated; or, at least, pay regards to the existence of pre-war conduct that consist of non-violent means (and does not amount to use of force). An exception is also made when discussing State sovereignty, where it is briefly investigated when a violation amounts to a conduct which triggers Article 51 of the UN Charter. Moreover, the thesis excludes civil war (non-international armed conflict, or NIAC for short), as the aim and purpose of the thesis only involves the comparison of the legal frameworks pertaining to peacetime and warfare. Thus, the thesis only regards inter-state relations in its application, analysis and final conclusions.

[9] In this thesis, the use of terms such as "gaps" or "gray areas" only refers to the problems which hybrid warfare creates in the unregulated area of jus ante bellum.

1.3 Methodology and material

Since the main purpose of the thesis is to conceptualize Hostile Attritional Operations (HAO:s, i.e. non-violent, pre-war conduct and hybrid warfare in the form of cyber attacks and information influence operations, aimed at the attrition of State) as a jus ante bellum concept, the method applied and sources used has to be aimed at fulfilling this purpose. In addition, the research questions also affect the methodological approach and the selected material which processes the material at hand. However, the approach of the thesis cannot deviate from the accepted and established hierarchies and methods of public international law, and the thesis has to be adapted to and proceed from the established methodological ways of public international law.[10] To accomplish this, the thesis takes its departure in Article 38 of the International Court of Justice (ICJ) Statue, which is considered an authoritative enumeration of the legal rules of public international law.[11] Article 38 is therefore of essence in the understanding of the subject, methodologically as well as materially.[12] In connection to this, an attempt is also made to relate its content into the context of this thesis and its subject of hostile attritional operations.

Article 38 consists, as mentioned, of an authoritative enumeration (however, not considered exhaustive) of the sources of public international law, which is often turned to in order to decipher the content of the latter.[13] The Article differentiates between four categories of sources: a) international conventions, b) international customs, c) general principles pertaining to international law, and d) judicial decisions and the "most highly qualified publicists of the various nations", as well as between primary (conventions, custom, and general principles) and secondary/subsidiary (judicial decisions and the works of scholars) sources.[14] When navigating Article 38(1), it is also necessary to be aware of what is considered to be the hierarchy of international law, consisting of *jus cogens* (primary, binding obligations that States cannot deviate from, regardless of its obligations to other international law),[15] *erga omnes* (obligations that all states have an interest of fulfilling its part of),[16] and

[10] What constitutes the accepted hierarchy of international law is, in some aspects, debated, see Crawford, 2019, pp. 19–20; Shaw, 2021, pp. 104–109.
[11] Shaw, 2021, p. 59. The use of the term legal *rules*, instead of legal *sources*, has to do with the fact that Article 38(1) does not *directly* treat legal sources, even though it appears implicitly, Bring et al., 2020, p. 30; Crawford, 2019, p. 20 However, other scholars still use the term sources when referring to Article 38(1), see e.g. Shaw, 2021, pp. 58–59; Henriksen, 2017, p. 23.
[12] Besides the fact that there are discussions of the ICJ Statute's "complete statement of the sources of international law", there are also concerns on whether the enumeration in Article 38(1) constitutes a falling hierarchy, see e.g. Crawford, p. 20; Henriksen, 2017, pp. 34–36.
[13] Bring et al., 2020, p. 29.
[14] Henriksen, 2017, p. 23.
[15] Henriksen, 2017, p. 36; Shaw, 2021, pp. 104–109.
[16] Oxford Reference, *Erga omnes obligations*, available via [https://www.oxfordreference.com/display/10.1093/oi/authority.20110803095756413], accessed 2024-10-13.

Article 103 of the Charter of the United Nations (UN Charter), which states that States' obligations under the UN Charter has precedence over other international obligations.[17] Additionally, it is important to be conscious of *lex specialis*, i.e. the tenet of specific law having primacy over general law, when mapping out the method and relevant regulations of the subject matter at hand.[18] Lex specialis is, for example, relevant when navigating the frameworks of IHL and IHRL.[19] Another issue is the problem of fragmentation of international law; what is holding (public) international law together?[20] These are not easy questions to have answered, and are intrinsically part of the problem which the phenomenon of HAO:s poses. As will be shown, however, there are authoritative international documents which can help in the interpretation of the connectivity between the different legal "areas" of international law, as well as turning to Article 31(3)(c) VCLT and the principles of systemic integration when interpreting the relation between treaties.

Before proceeding with this in mind, and returning to apply this methodological approach to the specific subject matter of the thesis, a general statement that can be made is that public international law is mostly built upon international custom and treaty law.[21] This is, as mentioned above, also reflected in Article 38(1), beginning in its first enumeration 38(1)(a), with a wording that reads that the court shall apply "international conventions, whether general or particular, establishing rules expressly recognized by the contesting states". In other words, it informs us that treaties constitute such a primary source in international law, since it is considered to be the firsthand and most obvious way to establish rights and obligations in international relations.[22] Treaties can be presented in the form of Conventions, Charters, Protocol and Declarations, among others,[23] and are divided into two types of treaties; *law-making treaties*, which often are more general in nature and occurring in multilateral treaties, and *contract-making treaties*, with which is referred to when regional and bilateral treaties with more specific content.[24] The latter concerns, for instance, *International Covenant on Economic, Social and Cultural Rights* (ICESCR).[25] A special status holds, as mentioned, the UN Charter (formally, a multinational treaty) as it according to Article 103 in

[17] Sthoeger (2024), "Article 103 of the United Nations Charter: Uncharted Possibilities? The Ukraine Conflict and beyond", in *Mich. J. Int'l L.*, 45, p. 153.
[18] Bring et al. 2020, p. 32. Lex specialis (derogat legi generali) does, however, not take precedence over what is considered jus cogens rules, Shaw, 2021, p. 105; Bring et al., 2020, p. 18.
[19] See e.g. Katz, 2021, p. 666.
[20] See also Shaw, 2021, pp. 54–55.
[21] Weissbrodt and de la Vega, 2007, p. 4; Bring et al., 2020, p. 30.
[22] Henriksen, 2017, p. 23. In this context, it is important to note (as is mentioned earlier in this section) that the content of treaties cannot be given primacy over rules of jus cogens character, see Shaw, 2021, pp. 104–109.
[23] Dinstein, 2004, p. 7; Bring et al., 2020, p. 30, 45; Svanberg, 2015, p. 13; Chinkin, 2010, p. 105.
[24] Bring et al., 2020, p. 30.
[25] See, regarding the issue of all States not being part of ICESCR, in the Tallinn Manual 2.0, 2017, "Part II Specialised regimes of international law and cyberspace/6. International Human Rights Law", para 2.

which, as mentioned above, demands are made on the States to hold its obligations under the Charter above its other international dittos.[26] As has been mentioned above, the problem of fragmentation of international law also poses a problem when trying to achieve a conceptualization of HAO:s, something that will be apparent below.

In this thesis, several treaties are actualized and thus naturally included; the most obvious one perhaps being the UN Charter, alongside the obvious central treaty for the method and material which is the Statute of the International Court of Justice (ICJ). Regarding the peacetime regulations, which will be examined in relation to its handling of HAO:s, less treaties are of relevance, but other subsidiary sources are actualized, which will be reviewed and clarified below. Concerning LOAC, there are several treaties that are actualized by the question of jus ante bellum and HAO:s. Of not insignificant relevance for the thesis are also the four Geneva Conventions, as well as the two Hague Conventions from 1899 and 1907. Here, the Commentaries of the International Red Cross (ICRC) have been useful in determining the meaning of the content of the Geneva Conventions and its additional protocols (AP:s). Of particular interest in this context is article 37 in the additional protocol I (AP I), which regulates the prohibition of perfidy and in article 37.2—more specifically, which constitutes an exception where, inter alia, ruses of war are regulated. Treaties regulating International Human Rights Law (IHRL), which is a part of LOAC and which the States has to relate to,[27] are first and foremost ICESCR and *International Covenant on Civil and Political Rights* (ICCPR); these are used when dissecting the legal framework of armed conflict pertinent to HAO:s.

Continuing on to the next enumeration of Article 38(1)(b), where it is said that "international custom, as evidence of a general practice accepted as law" is a source of international law that the Court *shall* apply. International custom is a more debated legal source, at least in comparison to treaties.[28] Unlike the making of treaties, international custom does not need the signing of a written document, but develops through a combination of State practice and opinio juris.[29] It is, nonetheless, of immense importance for international law, not at least when there is a lack of convention or treaties dealing with the topic of so-called hostile attritional operations (HAO), i.e. in the form of cyber attacks and information

[26] Hill et al., 1996, pp. 6–7; Wrange, 2015, p. 86. However, as mentioned in *supra* note 22, treaties can never be given primacy over such rules which constitute *jus cogens*, i.e. peremptory rules which States are unable to deviate from, see Henriksen, 2017, p. 36; Shaw, 2021, pp. 104–109.
[27] Weissbrodt and de la Vega, 2007, pp. 6–8.
[28] See Shaw, 2021, p. 62, 78.
[29] Regarding treaties, see Svanberg, p. 13 f.f.

influence operations, as cyber attacks are less regulated in treaties.[30] The elements of custom have been articulated by Crawford as consisting of *duration and consistency of practice*, *generality of principle* and the tenet *opinio iuris sive necessitatis*.[31] Custom concerns a lot of the material used in this thesis, one of them being cyber operations (or attacks), which is very sparsely directly regulated in treaties, and little "cyber-specific" custom have been developed.[32] However, the fact that States have expressed that international law is applicable to cyberspace and such information and communication technology which this thesis is aimed at is taken note of and, going forward, discussed as States having given evidence of "general practice accepted as law".

In the following enumeration, Article 38(1)(c), it is stated that "the general principles of law recognized by civilized nations". General principles of law should not, as opposed to the sources which are treated in Article 38(1)(d) (see below), be considered a "subsidiary source".[33] This enumeration applies to the thesis regarding i.a. the principles bona fide and pacta sunt servanda (approximately "agreements shall be kept"),[34] which constitutes foundations of the principal presumptions upon which public international law is built.[35] General principles of law can also be used to interpret the meaning of treaties when it is needed.[36] With other words: principles of law provides a background to why the regulations have been modeled in the way they are (*ratio legis*).[37] To get a full understanding of the tenets which are coining public international law and its modeling, especially in relation to the subject at hand, some of them are given a short outline in the initial Chapter of the thesis' descriptive parts.[38]

In the last enumeration, Article 38(1)(d), it is said that the court shall apply "subject to the provisions of Article 59, judicial decisions and the teachings of the most highly qualified publicists of the various nations, as subsidiary means for the determinations of rules of law". In this regard, it is important to note the mention of Article 59 which makes clear that judicial decisions are not binding for anyone except the parties involved; however, the Court often follows its settled jurisprudence and declared in *Application of the Genocide Convention* that

[30] See e.g. "Introduction", *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, February 2017, p. 3.
[31] From here on out referred to as "opinio juris". Regarding customary law, see Crawford, 2019, pp. 21–28.
[32] Custom is nowadays undoubtedly *applicable* to cyber and information and communication technology (ICT), even though it is hard to single out any definitively "cyber-specific customary international law", see "Introduction", in *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, February 2017, pp. 3–4.
[33] Regarding opinio juris, see Crawford, 2019, pp. 23–25.
[34] Crawford, 2019, p. 434. This is also considered to be a part of customary law, Bring et al., 2020, p. 18.
[35] Bring et al., 2020, p. 33.
[36] ILC, A/CN.4/L.702, 2006, p. 15.
[37] Ramberg et al., 2024, p. 85.
[38] See section 3.2 below.

it would not deviate from it, only should "very particular reasons" demand it.[39] Furthermore, even though judicial decisions only bind the subjects to the ICJ decision, the decisions can *become* customary law by States expressing that they view it as such.[40] This source of international law is naturally occurring in the thesis, with most of the material stemming from the International Court of Justice (ICJ)[41] and its predecessor, Permanent Court of International Justice (PCIJ).[42]

As regards the last enumeration, "the teachings of the most highly qualified publicists of the various nations", i.e. doctrine, it is also considered to be a subsidiary source of international law.[43] However, doctrine is often used as references in court, and therefore often gets a de facto influence.[44] In order to give a background and to describe international law in the areas specific to this thesis, the works of some established authors have been consulted, both in general public international law and the specific areas of which are the subject matter of the thesis, i.e. the frameworks of peacetime and armed conflict, pertinent to such hybrid warfare that bears the character of cyber operations and information influence operations. The most central treatise used in this thesis is the Tallinn Manual (2.0), which contains the settling down of lex lata by experts in the cyber area. The authority of the Manual should, according to the authors themselves, be understood as opinions by the two International Groups of Experts having authored it, but at the same time meant to reflect the law "as it is" (lex lata).[45]

At least as equal to the teachings of qualified publicists are the contributions of the International Law Commission (ILC).[46] Some of the reports used in this thesis which has been presented by ILC, such as *Fragmentation of International Law: Difficulties Arising from the Diversification and Expansion of International Law* and *Articles on Responsibility of States for Internationally Wrongful Acts* (ARSIWA), classify as such a material fitting within this category of sources.[47] These documents serve as codification of international law, which, according to Crawford, partly consist of the "comprehensive settling down of the lex lata".[48]

---

[39] *Application of the Genocide Convention* (Croatia v. Serbia), ICJ Reports 2008, General List No. 118, 18 November 2008, pp. 412, 428–429. See also Shaw, 2021, pp. 92–93.
[40] Generally regarding States' making of customary, see Solis, 2022, section 1.3.6, p. 16.
[41] See e.g. *Nicaragua Case* (Nicaragua v. United States of America), ICJ Reports 1986; *Prosecutor v. Tadić*, ICTY Case IT-94-1, ILM, vol. 38; ICTY, *Prosecutor v. Naletilić and Martinović* (Judgement). Regarding PCIJ, see Henriksen, 2017, p. 6.
[42] Even though the latter is no longer existing, its legal cases still have an impact on international law, especially its landmark case Lotus, which is of importance to this specific thesis, see *S.S. "Lotus"* (*France v. Turkey*), Judgement No. 9, PCIJ Series A No 10, ICGJ 248 (PCIJ 1927), see further in Chapter 3.
[43] Crawford, 2019, pp. 40–41.
[44] Crawford, 2019, p. 40.
[45] *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2017.
[46] Henriksen, 2017, pp. 32–33.
[47] Crawford calls this "other material sources", see Crawford, 2019, p. 39.
[48] Crawford, 2019, p. 41.

Its drafts—especially concerning ARSIWA—often gain the recognition of e.g. international courts as an authoritative source of international law.[49]

Concludingly, some last methodological concerns specific for this thesis needs to be addressed. With the aim of the thesis in mind, the examination is to a large extent explorative; certain concepts of public international law are "tested" against the ditto, in order to examine whether there are uncertainties or lackings in the handling of non-violent, pre-war conduct of attritional nature. Moreover, this examination is conducted on a systemic level, which means that certain aspects of the varying regulations of peacetime and armed conflict have been chosen by its perceived relevance for the problem of HAO:s.[50] This approach is inherently associated with risks of the examination in question being incomplete or lacking in certain regards; however, the goal is to be transparent with such issues in cases of occurrence.

1.4 Theories of international law

Having outlined the methodological approach applied to the thesis, a shorter theoretical background of the topic at hand is in place, as theory to a larger extent than in other legal areas is needed to understand public international law.[51] The main aim and purpose of this thesis is to conceptualize Hostile Attritional Operations (HAO:s) as a jus ante bellum concept, and the theoretical anchoring must be modeled with this in mind. Additionally, it is in place to remind the reader that both lex lata and lex ferenda arguments will occur throughout the thesis—especially in its analytical parts—why different theoretical applications have to be taken into consideration. Issues pertinent to this question will be briefly discussed in this section, while making an attempt to explain its application on the thesis as a whole.

Theory wise, international law has historically been coined largely by natural law, but legal positivism has also had a great impact on its forming.[52] The influences of legal positivism are not least of relevance when discussing sources of public international law, and especially Article 38(1) of the ICJ Statute.[53] The theory of legal positivism has been discussed, dissected and elaborated on by a number of international scholars, which since have been contributing to and criticizing the works and thoughts of previous scholars. One of

[49] Crawford, 2019, p. 41.
[50] The assessment of the principle of sovereignty and non-intervention being most relevant for the problem of HAO:s pertaining to peacetime is one example of this; another is the examination of International Human Rights Law (IHRL), where the "explorative" character of the thesis is especially apparent.
[51] Bring et al., 2020, p. 35.
[52] See D'Amato, 2010, pp. 1–2; Bring et al., 2020, pp. 35 f.f.; Shaw, 2021, pp. 18, 20–22, 41–45.
[53] Since Article 38(1) in the ICJ Statute is considered the most authoritative attempt at listing the sources of public international law, it can therefore be claimed to also be the most established guideline on determining *lex lata*, see Bring et al., 2020, p. 39 f.f. See also Shaw, 2021, pp. 38–39.

the definitions of legal positivism is "[…] a legal theory of law where international law is strictly seen as a unified system of objective rules based on the collective will of States".[54] This is the same definition of positivism which this thesis is based on. The use of legal positivism can be claimed to be helpful when trying to determine the applicable law to a certain research question, which is also how Article 38(1) in the ICJ Statute is designed to be used as.[55] This is of utmost importance for the methodological and material approach when navigating international law. Further, and as mentioned, the theory of legal positivism influences the way in which the applicable international law is identified and applied, and is thus connected with both the descriptive parts and occurring lex lata arguments of the thesis.[56]

1.5 Previous research pertinent to Hostile Attritional Operations

The thesis consists of a couple of different areas of (public) international law, namely the respective regulations of peacetime and armed conflict as it pertains to HAO:s. Herewithin, there are certain terms and concepts which have been coined and developed by other authors, that requires recognition and a review of what has already been accomplished in the areas of public international law which is the subject of the thesis.

Since this thesis dwells on cyber attacks and information influence operations which takes place on the internet (or "in cyberspace"), the settling of lex lata in the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2017), which examines the regulations and handlings of cyber operations in regards to both peacetime and armed conflicts, has been of ample use. This work is to a large extent consulted in regards to the handling of cyber attacks and information influence operations concerning violations of State sovereignty, non-intervention and State responsibility in peacetime, as well as violations of IHL and IHRL during armed conflict. This examination is a keystone in later being able to analyse HAO:s conducted on the internet.

Furthermore, the subject of information or communication influence within the application of IHL has been processed and introduced in a thesis by Pontus Winther in 2019, where the author outlined the legal framework lex lata with legal positivism as a starting point.[57] In his thesis, Winther coined the term *communication influence activities* to be used

[54] Winther, 2019, p. 47 with references (especially f.n. 106). For an account of *classical* legal positivism as opposed to *modern* legal positivism, see Wacks, 2021, pp. 74–141. Regarding natural and positive law in public international law, see Shaw, 2021, pp. 41 f.f.
[55] Winther, 2019, pp. 46–47.
[56] However, per the aim of the thesis, it also includes lex ferenda arguments, which are not restrained by theories mentioned in this section.
[57] Winther, Pontus, *International Humanitarian Law and Influence Operations*, 2019.

for research conducted within the scope of IHL. The term, which Winther phrases as "the use of methods and means of communication by which information is disseminated from one actor to another in order to influence the persons, attitudes or behavior of the latter"[58] was designed for his specific dissertation.[59] In this thesis, a similar term is used, with a slight modification of the meaning and wording of the concept, namely *information influence operations*. Here, a State actor with malicious intent is presumed to be the sender of the information in question. The term is, in addition, intended to constitute one of two components of the overarching term *hostile attritional operations* (HAO:s),[60] and has been accommodated to fit the navigation between peacetime *and* armed conflict, thus, not being limited to either IHL or LOAC.

As regards the second of the two constituents of the concept of HAO:s, namely cyber attacks, it has been dealt with by a number of scholars. One of them is François Delerue (2020),[61] the work of which has been of great importance in the navigation of the peacetime regulations, especially pertaining to various forms of peacetime countermeasures.[62] Lastly, regarding jus ante bellum and aspects relevant to consider in the discussion in Chapter 5, Morten M. Fogt's (2020) article on building legal resilience in jus ante bellum has constituted helpful guidance.[63]

1.6 Structure and disposition

Beginning in Chapter 2, some central notions, as well as relevant terminology, are introduced and explained. In this context, concepts such as HAO:s, hybrid warfare, cyber attacks, information influence operations and non-violent, pre-war conduct will be elaborated on, and the theoretical lense of jus ante bellum is given a preface to its application on the thesis. In Chapter 3, the regulation of conduct pertinent to HAO:s in peacetime is outlined and analyzed, in order to get an understanding of in what way the current regulations and principles of international law in peacetime lacks efficiency and (or) in other ways does not

[58] Winther, 2019, p. 41.
[59] Winther leaves the reader with suggestions on further research that he identifies as needed in the area. As Winther has with his dissertation chiseled out a regulation pertinent to communication information activities, his suggestion is to apply this "in a more systematic manner in order to determine whether IHL provides civilians with sufficient protection from communication activities", see Winther, 2019, p. 392. Such a thorough attempt will not be made in the thesis.
[60] The precise content of the term will be defined and further elaborated on in Chapter 2 below.
[61] Delerue, *Cyber Operations and International Law*, 2020.
[62] See further Chapter 3; section 3.8 and subsections 3.8.1–3.8.3.
[63] Fogt (2020), "Legal Challenges or 'Gaps' by Countering Hybrid Warfare – Building Resilience in *Jus Ante Bellum*", in *Southwestern Journal of International Law*, Vol. XXVII:1.

suffice in the name of countering HAO:s. Here, the essence of the problem of HAO:s is also articulated and described.

Chapter 4 deals with the Law of Armed Conflict (LOAC), consisting of both International Humanitarian Law (IHL) and International Human Rights Law (IHRL). After having examined these respective regulations, the extent to which there is an unregulated "gap" or "gray area" that causes a disruption in countering HAO:s is discussed in Chapter 5, which also (and mainly) deals with the possible establishment of HAO:s as a jus ante bellum concept. In Chapter 5, the establishment and challenges of HAO:s as a jus ante bellum are also discussed, followed by an analysis of the result presented in the descriptive parts in Chapter 6. Lastly, in Chapter 7, some final remarks and conclusions are made, as well as putting forward suggestions on further research pertinent to the subject matter of the thesis.

2 Hostile Attritional Operations and other central concepts

2.1 The concept of Hostile Attritional Operations and its constituents

The primary aim of the thesis—being to conceptualize HAO:s as a concept of the not (yet) established legal area of jus ante bellum—demands an introduction to what is implied when referring to this very central and somewhat semi-novel concept to international law. Additionally, jus ante bellum as a legal area between peace and wartime will be further outlined and elaborated on below. It is important to yet again remind the reader that this approach is limited to examine the "gap(s)" or "gray area(s)" pertinent to the handling of HAO:s in the respective frameworks of peacetime and armed conflict.

Therefore, there is a need to begin the descriptive parts of the thesis with an introduction to Hostile Attritional Operations and its intended constituents, namely cyber attacks and information influence operations. It is also necessary to show how it relates to the already established concepts such as hybrid warfare and other public international law. As there are several concepts related to HAO:s that already exist in international law, the introduction of this new concept and its future existence will also have to be justified in this context. Furthermore, the question of whether some aspects of the armed conflict regulation can serve as templates for what a regulation of HAO:s in jus ante bellum could look like is also discussed and elaborated on. Lastly, some other central concerns, such as fragmentation of international law and commonly used terms in the thesis, will be introduced in the finishing sections of this Chapter.

2.1.1 Hostile Attritional Operations

Hostile Attritional Operations (HAO) is, as mentioned, a central concept that will be introduced and used in this thesis, and is designed by the author for this specific work. In essence, it refers to those activities that States and non-State actors perform against an aggrieved State, with the purpose of wearing down the State in question before or during warfare. Another concept that is closely related to the one of HAO:s is hybrid warfare. In this thesis, it will be used as a concept aiming towards defining the phenomenon of hostile States by prima facie non-violent means attempting to wear down the resistance of a State, whether that be democratic, political, military or civilian types of resistance.

To break down the concept further, *hostile*[64] refers to the intent; the actions must be taken with ill-intent towards the aggrieved State. *Attrition* refers to the way it wears down the aggrieved State in question, in a way that benefits the hostile-intended State's in an intended war. *Operations*, instead, refers to the way it is carried out, i.e. the activities must be performed in or during an organized, planned event. The activities intended to be examined are *prima facie* of non-violent nature, but can take the form of act or activities which still causes damage, in a more indirect or long-term way. The North Atlantic Treaty Organization (NATO) has, for example, pointed out Russia as responsible for hybrid activities—consisting of e.g. sabotage, acts of violence, cyber interference, disinformation campaigns—that NATO member countries have been exposed to, where the term *malign activities* is being used.[65] Other examples of different hostile acts (or activities) are cyber attacks that knocks out the power grid in a certain location of another State, causes malfunction in critical or closes down crucial payment systems in a State.[66]

Hostile Attritional Operations are, in this thesis, thought to consist of both cyber attacks and information influence operations. This requires different approaches, at least in some regards; however, a common denominator is that they are thought to take place in cyberspace. Cyber attacks are, as mentioned, not regulated to any greater extent in treaties, but have gotten the more impact in customary law.[67] Though not considered to constitute a strictly legal concept,[68] cyber attacks have been the subject matter for legislation, as well as scholarly works. HAO:s could technically consist of other activities, most obvious those that constitutes various forms of violent means, but as mentioned above in section 1.3, this thesis has been limited to only treat such HAO:s that *prima facie* consists of non-violent means (and, furthermore, only those that can be categorized as cyber attacks and information influence operations). These kinds of activities and acts will, as said, sometimes be referred to by the term *hybrid warfare*, which also will be dissected further under section 2.1.2.

In sum, Hostile Attritional Operations (HAO:s) can be said to constitute an overarching concept, covering both cyber attacks and information influence operations. Both

---

[64] Related terms are "hostile-intended", "unfriendly", "malign" or "malicious" activities, etcetera.
[65] See "Statement by the North Atlantic Council on recent Russian hybrid activities", published 2024-05-02, available via [https://www.nato.int/cps/en/natohq/official_texts_225230.htm?selectedLocale=en], accessed 2024-05-03; Colliver et al., *Smearing Sweden. International Influence Campaigns in the 2021 Swedish Election*, 2018.
[66] Examples of this can be bank systems, card payments in specific stores, or payment systems like, *inter alia*, the Swedish payment service "Swish" (or the Norwegian/Scandinavian payment service "Vips"), but also other bank functions that are used in the daily life of individuals in, and citizens of, a State.
[67] "Introduction", *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, February 2017, p. 3.
[68] Fogt writes about "Hybrid Threat or Warfare" as having become a "discourse concept", i.e. a "non-legal concept", see Fogt, 2020, p. 30.

of these components can be said to have a cyber dimension, in that cyberspace often is used to commit the act in question, whether it be a cyber attack or information influence operation, or if it is committed in a time of peace or during warfare. In essence, HAO:s refers to such hybrid warfare that consists of cyber attacks and information influence operation that is taken by a State towards an aggrieved State, and that is intended to harm the aggrieved State in question. It is therefore of relevance to also give an introduction to what is here referred to by *hybrid warfare*.

2.1.2 Hybrid warfare, lawfare and other terms for pre-war conduct

Hybrid warfare is a widely used term, not only in a legal context, which sometimes refers to a type of conduct where unconventional methods and means are being used as, within or during preparations for warfare.[69] It can also refer to a situation that categorizes as state somewhere in between peacetime and warfare, or to a situation that would amount to war or a war-like state, but cannot be proven to meet the criterias of war; at least not to such armed conflict which invokes the application of LOAC and IHL. The North Atlantic Treaty Organisation (NATO) has also touched upon this concept.[70] As the terminology varies,[71] hybrid warfare is a commonly accepted concept, however many non-legal connotations it may have.[72] Since the concept HAO to a certain degree overlaps what is sometimes referred to as hybrid warfare, it is necessary to discuss how the concept of HAO relates to the already established concept hybrid warfare and how the concept of HAO:s can be used to contribute to a further understanding of hybrid problems.

In the thesis, what is usually meant when referring to hybrid warfare is *unconventional methods and means being used as, within or during preparations for warfare*.[73] Notwithstanding this, the term hybrid warfare sometimes simply is used when referring to acts of war which cannot be attributed, especially when cyber operations and attacks result in concrete, physical damage which—if it had been accomplished by other methods or means—would have been considered an act of war. Since one of the aims of the thesis is to make a distinction between peacetime regulation and that of warfare, however, the thesis will focus on hybrid warfare in the sense of it being unconventional methods or means used as, within or during preparations for warfare.

[69] See e.g. Fogt, 2020, p. 37.
[70] See Fogt, 2020, p. 30 with reference (f.n. 3).
[71] See Fogt, 2020, p. 30.
[72] Fogt, 2020, p. 30.
[73] Fogt, 2020, p. 30.

As mentioned above, when navigating the legal framework of peacetime pertinent to hostile attritional operations (HAO:s), the term hybrid warfare is not used as a fully-fledged synonym to HAO:s. Instead, it refers to such a situation where it is unclear whether it is a question of an act of war or if the activity falls outside the definition of warfare, which is usually the case when such hostile attritional operations do not correspond to the definition of an act of war. When this occurs, it will be explained in more detail and motivated why it is done, to not confuse the reader. However, the term hybrid warfare is more commonly used in the context of LOAC and IHL, that is in Chapter 3, and the emphasis is thus (as said) to have been put on the implication of hybrid warfare as "unconventional methods and means are being used as, within or during preparations for warfare".

2.1.3 Cyber attacks (and/or operations)

Beginning with dissecting one of the two forms of Hostile Attritional Operations (HAO:s), namely *cyber attacks*, it is first important to note that it—at least according to some scholars—is not considered a legal term in its proper sense.[74] In fact, it has been discussed whether international law is suited to deal with cyber attacks,[75] which in and of itself is an aim of this thesis. Notwithstanding this discussion, the conclusion has still been made that international law applies to cyber attacks and other cyber-dimensional phenomenons.[76] This is because of the fact that cyber attacks (or operations) at least can be said to have a legal dimension,[77] as well as a lot of practical consequences within the context of international relations. Therefore, it is of interest to further investigate its implications on international law and whether it is necessary to regulate cyber attacks and operations further and in more detail. Another question of interest to discern is if the existing regulations in fact are enforced and—if not—what prevents effective enforcements.

In this thesis, the term *cyber attacks* (sometimes termed as *cyber operations*) refers to such operations which a hostile State exposes an aggrieved State to, and which are prima facie non-violent in the direct consequences which it renders. Some scholars have taken on the viewpoint of cyber attacks as measurements which do not harm *persons*, but instead "computers".[78] This assumption is not shared in the application of cyber attacks in the thesis, as it would go against the very idea behind the usage of a terminology like HAO:s, designed

[74] See Delerue, 2020, p. 38.
[75] Delerue, 2020, p. 1. See also Newton and May, 2014, pp. 266–267.
[76] Delerue, 2020, p. 1.
[77] See Delerue, 2020, p. 6.
[78] See e.g. Newton and May, 2014, p. 265.

to take aim at describing such long-term, attritional effects that prima facie non-violent hostile measurements like cyber attacks have on a State. In other words, it is in this context accepted that in order to explore and highlight these specific characteristics of HAO:s, one needs to consider the long-term effects when mentally mapping out the legal area of jus ante bellum.

Furthermore, in public international law, the addresserants are States and non-governmental organizations (NGO:s). However, in practice, the cyber attacks can take aim at both the State (like government websites), its civilians or systems that the society is in need of in order to function properly. This can be accomplished through, for example, so-called DDoS (denial-of-service) attacks by which the actor is causing an overload on a system, in order to cause disruptions in the function of the system in question. Margulies has—while examining the challenges of attribution and cyber attacks—differed between different types of cyber attacks: 1) DDoS attacks, 2) undermining of operating and 3) control systems,[79] the latter is sometimes categorized as "more serious" by some authors.[80] Here, different types of cyber attacks will be described when this is of relevance. DDoS attacks that consists of a mass of machines that uses its power to impair functions of the website that is the aim of the attack,[81] for example, are often aimed at causing an inconvenience, however temporary. Undermining of operating and control systems, instead, poses as a more permanent issue for i.e. the authorities or an otherwise crucial social function. An example of the latter is so-called syntactic attacks, that use malicious malware that is better known as "viruses".[82] There are also examples of States using cyber attacks to i.e. nuclear plants,[83] which pose a real danger both locally and regionally—sometimes even globally. Additionally, cyber attacks often consist of several stages,[84] which sometimes makes it harder to describe it in the terms of a HAO. However, in this thesis, the author will dwell on how cyber attacks in general *de facto* are being categorized and handled in the respective frameworks of peacetime and armed conflict, to illuminate any weaknesses when it comes to non-violent, pre-war conduct such as e.g. cyber attacks. Another important aspect of cyber attacks which is important to be aware of is the so-called "cyber security" debate, i.e. when governments infringes upon human rights (e.g. freedom of expression and freedom of association)[85] with

[79] Margulies, 2013, pp. 501–502.
[80] Margulies, 2013, p. 502.
[81] Margulies, 2013, p. 501.
[82] Margulies, 2013, p. 502.
[83] ICS Alert, "Cyber-Attack Against Ukrainian Critical Infrastructure", (last revised 20 July 2021), available via [https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01], accessed 2025-01-03.
[84] Margulies, 2013, p. 504.
[85] Fidler, 2014, p. 301.

reference to the cyber security of a State. This will be apparent and further discussed in Chapter 4 of the thesis.

As has been mentioned, the choice of including cyber attacks in the term Hostile Attritional Operations has been made on the basis of the nature of cyber attacks being prima facie non-violent. The presumption onwards is that these cyber activities, attacks or operations are *aimed at harming another State*, thus singling out unintentional activities. Cyber attacks and operations that are carried out with other motives than harming another State falls outside the application of this thesis.

2.1.4 Information influence operations

What historically has been referred to as propaganda is today often phrased as *information influence*, information warfare or lawfare.[86] The term *communication influence operations* has already been coined by Pontus Winther in his dissertation from 2019; here, the term is slightly modified to fit the aim and purpose of this specific thesis. Here, instead, the term *information influence operations* is used. It refers to such actions taken by one party with hostile intent toward an aggrieved party, as a means to the aim of weakening the aggrieved part in question.[87] Furthermore, it only aims at dealing with such hostile attritional operations that one State directs at another State's interests, even if it harms civilians and infrastructure on its way. Regarding information influence operations, however, it is important to note that it to a larger degree than cyber attacks consists of what some would call "psychological warfare".[88]

Furthermore—together with cyber attacks—these information influence operations are only viewed as part of a kind of non-violent so-called hybrid warfare, which can either be viewed as activities falling within the application of the regulation of peacetime, or one pertinent to that of law of armed conflict (LOAC) and international humanitarian law (IHL). Having previously discussed cyber attacks as one form of HAO, it can appear as if information influence operations are—in nature—so different from cyber attacks that it is irrelevant or difficult to conceptualize in the same kind of terminology. This is nevertheless not the case. As regards information influence operations, when taking the form of i.e. propaganda and deliberate spreading of misinformation that is directed at the citizens or combatant of an aggrieved State, they are often more abstract in nature and can be harder to

[86] See e.g. Fogt, 2020, p. 31.
[87] Winther has coined the terminology of "communication influence activities", the meaning of which is close to that of "information influence activities" used in this thesis. Winther's work is further discussed in section 1.5 above.
[88] See e.g. Winther, 2019, p. 23.

pinpoint as a HAO in comparison to cyber attacks, that not seldom causes damage that are measurable in a more concrete way (i.e. by hindering customers from using payments systems which makes them unable from obtain viands, causing damage on power grids in an area that affects the local populations' abilities from warming up their homes, etc.). This is why these different kinds of hybrid warfare—notwithstanding that they are both categorized as "hostile attritional operations"—sometimes are treated separately throughout the thesis. When this occurs, it will be clear to the reader by an explanation as to why it is done.

Information influence operations is a semi-novel concept, however the core aim of the operations or activities have been used for centuries. It can be claimed that propaganda has been, and still is, one of the most useful ways to influence others to feel, think and thereby influence the world view of the receiver in certain ways.[89] Recently, due to the developments of technology of modern days, it is easier than ever to get information across to the desired audience, however true the information that is being distributed may be. Social media forums such as TikTok, Instagram, Twitter (now X), Facebook and Telegram are a few such platforms that are known to distribute and, with the help of algorithms, present or distort information containing political angles and views with the purpose of manipulating perceptions, world views and opinions, etcetera.[90]

As previously mentioned, a term recently coined by Winther in his dissertation from 2019, is (unlawful) communication influence activities.[91] The problem arises from States with hostile intentions being able to use technology more efficiently today, in order to distribute modern day propaganda, and by doing so influencing citizens of a State—as well as politicians in higher office—in decision-making, vote casting in elections, and so forth.[92] This can involve using social media to spread what is sometimes called "fake news" in order to inter alia influence public opinion and higher-level political decision making. Obviously, this can be a way for hostile-intended States to influence and harm foreign democracies, which has been a very real worry for western States.[93] Wheatley (2020) words the objectives of

---

[89] NBC News, "TikTok says it's not spreading Chinese propaganda. The U.S. says there's a real risk. What's the truth?", 2024-09-16, available via [https://www.nbcnews.com/investigations/tiktok-says-not-spreading-chinese-propaganda-us-says-real-risk-rcna171201], accessed 2025-01-04.

[90] Generally, see e.g. Wheatley (2020), "Foreign Interference in Elections Under the Non-Intervention Principle: We Need to Talk About 'Coercion'", in *Duke Journal of Comparative & International Law*, Vol. 31:161.

[91] Winther, *Information Influence Operations and Influence Operations: The Protection of Civilians from Unlawful Communication Influence Activities during Armed Conflict*, 2019.

[92] Regarding intervention in election processes, e.g. Wheatley (2020), "Foreign Interference in Election Under the Non-Intervention Principle: We Need to Talk About 'Coercion'", in *Duke Journal of Comparative & International Law*, Vol. 31:161.

[93] See further in Katz, (2020) "Liar's war: Protecting civilians from disinformation during armed conflict", in *International Review of the Red Cross*, vol. 102(914).

information influence operations as "[aimed at creating] decision-making paralysis and/or to shift the policy position of the target so it comes to align with the interests of the foreign power".[94] This assumption of the intent behind conducting these kinds of information influence operations is what the examination in this thesis will relate to, going forward.

2.1.5 (Prima facie) non-violent means and pertinent concerns

In this thesis, Hostile Attritional Operations (HAO:s) are always thought to be an act of a State, a State actor or a natural person that does not amount to an act of war in its proper sense; i.e. there is no *prima facie* use of violence. This is due to the fact that the definition of what constitutes an act of war is relatively clear, as it requires that the action taken is a violation of the prohibition of violence.[95] Therefore, there has to be a mention that use of force, as it is stated in the UN Charter, is a term overlapping with "intervention". It is also important to take note of the fact that there are several terms pertinent to violence and use of force, like (an) *attack* and the concept of *aggression*, which are even narrower in its respective application.

As regards use of force, the term has a more narrow application than intervention; the latter does not require actual use of force, as do the former term according to the UN Charter.[96] As the Charter's article 2(4) states, "[a]ll member shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations". The violence that is intended with this phrasing is military violence, not economic or political dittos.[97] Nonetheless, a review of what is applicable and not to the specific problems with HAO:s is in its place, why the UN Charter and the different forms of prohibited means are included in the thesis (even though the author mostly refrains from treating the prohibition of violence, since this is not applicable on HAO:s per its definition). In the thesis, *intervention* and the prohibition of it will naturally be treated in the context of non-intervention, as it is viewed as part of a violation of the sovereignty of the aggrieved State in question. As intervention is also prohibited, a context will be given to the legal framework pertinent to non-intervention.

---

[94] Wheatley (2020), "Foreign Interference in Elections Under the Non-Intervention Principle: We Need To Talk About 'Coercion'", in *Duke Journal of Comparative & International Law*, Vol. 31:161, p. 193.
[95] See Bring et al., 2020, p. 190.
[96] Bring et al., 2020, p. 190.
[97] Bring et al., 2020, p. 190.

2.2 Jus ante bellum in context

2.2.1 Why a "jus ante bellum" approach?

Regarding what is considered "regular" warfare, there are typically two distinctions made when it comes to determining the set of rules applicable to the situation at hand. First, rules and principles pertinent to *jus ad bellum* set forward when it is legitimate to wage war,[98] second, *jus in bello* regulates the conduct of warfare, i.e. when war already is a reality.[99] However, hybrid conduct of States that consists of cyber operations and information influence operations (which in this thesis goes by the name Hostile Attritional Operations, HAO:s) usually takes place before a war, technically, is a fact.[100] In addition, for jus ad bellum to come into question, it requires that the use of force as well as the justification grounds for self-defense, which are found in the UN Charter's Article 51, are at hand.[101]

Hence, it is difficult to apply the principles of jus ad bellum and jus in bello to activities that a) are not violent in nature and, thus, does not qualify as an act of war, and b) (as said) usually takes place before the state of war is a fact. Neither the UN Charter, nor the four Geneva Conventions, are applicable on such acts performed by a hostile State. Thus, there is a need to turn elsewhere in search for applicable principles and regulations that can help counter the problem of hostile attritional operations. The term *jus ante bellum* can be said to refer to principles and international regulations of the situation that transpires *before* war has erupted.[102] According to Farrell, the term refers to "the justice of actions taken prior to the outbreak of hostility, with particular emphasis being given to the fostering of just societies and proper relations."[103] Looking at the common denominator in these descriptions of the concept, jus ante bellum can be understood as taking aim at constructing rules for pre-war conduct. A development of jus ante bellum has been proposed by scholars of international law who are focusing on hybrid warfare.[104]

What, then, can a jus ante bellum approach to HAO:s contribute to? Should pre-war conduct take aim at preparing for war, or preventing war? It can be argued that both fit within a proposed principle complex of jus ante bellum, even though international law, at least as it

---

[98] Bring et al., 2020, pp. 184–185.
[99] Bring et al., 2020, p. 185. Other sectioning of war-like situations are, e.g., jus *post* bellum and jus *contra* bellum, see regarding jus post bellum Fogt, 2020, p. 28; regarding jus contra bellum, see Delerue, 2020, p. 275 and below in section 2.2.2.
[100] See, generally, Fogt, (2020), "Legal Challenges or 'Gaps' by Countering Hybrid Warfare – Building Resilience in Jus Ante Bellum", in *Southwestern Journal of International Law*, pp. 28–100.
[101] Bring et al., 2020, p. 192–193.
[102] Brown and Bohm, 2016, p. 902.
[103] Farrell, 2013, p. 19.
[104] For example, see Fogt, "Legal Challenges or 'Gaps' by Countering Hybrid Warfare – Building Resilience in Jus Ante Bellum", in *Southwestern Journal of International Law*, 2020.

regards to peacetime, must take aim at protecting the peace. In this thesis, the jus ante bellum approach is proposed to first handedly serve a normative function, in that it is used to suggest a possible development in the area of HAO:s within public international law by attempting to show how HAO as a jus ante bellum concept can help highlight the attritional conduct which hostile-intended States are engaging in, to gain military advantages later on.

2.2.2 Jus *ante* bellum versus jus *contra* bellum – is there a need for both?

Having argued that the purpose of jus ante bellum must contain a strive for providing rules which exceedingly seeks to protect the peace, the academic existence of jus contra bellum—i.e. rules which take aim at protecting international peace—have to at least be mentioned and touched upon, in some regard. If jus ante bellum and jus contra bellum share the same purpose, i.e. the strive for preserving international peace, is it at all necessary to introduce yet another concept in international law, which risks complicating the navigation of international law further? That would perhaps be the case if the purpose of jus ante bellum *strictly* took aim at preserving international peace. It is here argued that, in jus ante bellum, there is a presumed assumption of at least one State already acting as if war is imminent, and by using non-violent (although invasive) measurements preparing for waging regular warfare in a near or semi-near future. It is further argued that rules pertinent to situations in jus ante bellum are modeled with the awareness of hostile-intended States using these kinds of measurements, and the recognition that war sometimes can and need to be prevented by using other means than diplomatic relations between States. Thus, rather than strictly looking to "cool down" a brewing conflict by looking to e.g. the UN Security Council to solve problems that can be categorized as pertinent to collective security,[105] jus ante bellum allows non-violent self-defense for an aggrieved State in the event of a violation, whether that be of its sovereignty, its right according to the principle of non-intervention, or the perseverance of peace.

[105] Regarding problems and lacks pertinent to the function of the UN:s Security Council, see e.g. Byers, 2005, Part One, pp. 13–50.

2.2.3 Challenges and controversies associated with applying a jus ante bellum approach

A jus ante bellum approach is neither unproblematic nor uncontroversial, and that is for several reasons. First off, as mentioned, it is not undisputed whether the existence of jus ante bellum principles are at all aspirational.[106] One critique of suggesting a jus ante bellum development is that the use of a jus ante bellum approach could be criticized for overlapping the regulated area of jus *ad* bellum.[107] An overregulation is therefore not desired, if not for fragmentation reasons, also because it is, in fact, unnecessary.

When suggesting an expansion of international law in connection to warfare regulations, it is important to keep in mind the historical fact which is that several wars have started by unintentional escalations, stemming from assumptions about another State's (hostile) intentions, inter alia.[108] The act of one State armoring its own military forces leading to a spiral which carries with it unforeseeable risks to the international peace and global (or regional) security situation could also be considered common knowledge by now. Thus, expansion of regulations that are associated with such effects will also always be an act of balancing States interest of maintaining its defense capability on the one hand, and protecting international security on the other; at least if done responsibly. Examples of possible dangers associated with suggesting extended abilities for an aggrieved State to respond to information influence operations or cyber attacks can thus be that a hostile State in its turn considers itself aggrieved, threatened or even decides to take the response as an invitation to further escalate the situation (which may have been the plan, all along).[109] Another challenge with an expansion of international law in jus ante bellum poses the issue of fragmentation of international law, which will be discussed further below.

2.2.4 Fragmentation of international law and jus ante bellum

Fragmentation of international law has already been discussed as a methodological problem, but it also has direct ties to the proposal of an expansion of international law in jus ante bellum. Fragmentation of international law has been dealt with by the International Law Commission (ILC) in their report from 2006, and is considered to have to do with the fact that

[106] See, for example, the discussion reproduced in Wertheimer, 2015, pp. 54–66.
[107] Brown and Bohm, 2016, p. 903. See also the discussion in Chapter 4 below.
[108] There are also plenty of examples of "war scares" that could have ended in a conflict of international dimension, but thanks to diplomacy, and sometimes sheer luck, did not, see e.g. Bring et al., 2020, pp. 182.
[109] This was the case in Eastern Ukraine long before the full scale invasion of February 2022, see e.g. Bring, *Anfallskrigens argument: Konsten att rättfärdiga våld*, 2022, Chapter "Putin och Ukraina", pp. 182–188.

international law has increased exponentially during the 2000th century, and especially with it being accomplished in a disorganized manner.[110] Legal areas pertinent to human rights, security, commerce and to address certain technological issues have been aimed at solving a certain problem at hand, and not at producing or being a part of the cohesive global order that is international law.[111] According to the ILC report, some scholars have put forth the concern of the fragmentation problem as having repercussions on the retention of the structures of international law, causing it to undermine the structure and functions of general international law, inter alia.[112]

For HAO:s and the proposed legal area of jus ante bellum, the problem of fragmentation of international law is in no way irrelevant. One issue is based on the concern of the increasingly sorely task of navigating and integrating the different legal areas, but also the strict differentiation between peacetime and warfare, causing some pre-war conduct of hostile and preparatory nature to "fall through the cracks". One ambition of the work that is this thesis is in part to, by illustrating the problems of HAO:s, contribute to "bridging the gap" between peacetime and armed conflict and by doing so, in turn, contributing to the counteracting of some of the problems arising from the fragmentation of international law. This cannot be done without looking at the research that has been made on how to solve fragmentation related dilemmas, as well as assessing the width of the fragmentation and the extent to which it is relevant for jus ante bellum and HAO:s.

2.3 Lending of the Law Armed of Armed Conflict as a template for the modeling of jus ante bellum and Hostile Attritional Operations

In this thesis, the regulations of law of armed conflict (LOAC) are outlined in regards to its application on HAO:s. This is, in part, done to show the "gap" or "gray area" which is presumed to exist between the peacetime and armed conflict regulation. However, the LOAC regulation serves another purpose, and that is to serve as a model for how certain aspects of the handling of HAO:s can be lended into the development of jus ante bellum and the phenomenon of HAO:s. Even though the thesis does not primarily set aim at bringing suggestions on what a concrete development of jus ante bellum should look like, some aspects of the handling of HAO:s in armed conflict can be useful to illustrate the problem of hostile attrition, since cyber attacks and information influence operations also occurs within and as a

[110] ILC, A/CN.4/L.702, 2006, pp. 3–4. See also Shaw, 2021, pp. 54–55.
[111] ILC, A/CN.4/L.682, 2006, p. 4. See also the discussion in Shaw, 2021, p. 58–59.
[112] ILC, A/CN.4/L.682, 2006, p. 4.

way of doing warfare. Examples of such are the handling of ruses, perfidies, cyber attacks that amount to "attacks" according to LOAC, etcetera, and has to at least be mentioned in this context. This approach will be clarified in Chapter 4 and 5, but it deserves a shorter mention and clarification in this section as well.

2.4 Other central terminology and some common abbreviations

Above, some central concepts to the thesis have been established, dissected and elaborated on. Lastly in this chapter, some clarifications on and modifications of commonly used legal terms within the area of international law deserves some clarification. When the term *international law* is used in this thesis, it refers to *public international law*, although sometimes the entire term is worded out.[113]

Furthermore, when using the term Law of International Armed Conflict (LOAC), it often includes the application of International Humanitarian Law (IHL). In this specific thesis, when the LOAC term is used, it refers to the legal area that applies to a conflict which has already broken out. Therefore, it almost always is replaced by, or used synonymously with the term IHL. The aim of the legal area which is IHL can, according to Nils Melzer, be defined as "to restrict the means and methods of warfare that parties to a conflict may employ and to ensure the protection and humane treatment of persons who are not, or no longer, taking a direct part in hostilities"[114], and it is this aim which is implied when discussing pertaining questions in regards to IHL. However, LOAC can also refer to the laws applicable to only adversaries or combatants, why the attempt to differ between the two terms is made, when necessary and possible. In this thesis, LOAC also includes International Humanitarian Law (IHRL), which will be clear throughout the thesis.

[113] Which is a common abbreviation of *public international law*, see for example Henriksen, 2017, p. 1, f.n. 1.
[114] Melzer, 2016, p. 17.

3 Hostile Attritional Operations in peacetime

Public international law is generally considered to be the structure to which we look for meddling in international relations, and is generally perceived as a tool used exceedingly in the strive to protect peace and stability.[115] However well international law in general fulfills its perceived task, it is still the reality in which States operate, and members of the international community have committed themselves to be bound by certain norms and rules both in peacetime and during armed conflict.[116]

While the regulations of HAO:s in both peacetime and armed conflict can appear quite clear when interacting with the respective regulation, there are what one can call "gray areas" or "gaps" where the regulations viewed as a whole are, at best, patchy. Hybrid warfare, and its many names,[117] in the form of cyber attacks (or cyber *operations*) and information influence operations, can be executed in and under a wide range of scenarios and conditions, including during peacetime. One question consists of whether the law of armed conflict (LOAC) regulation "takes over" where the peacetime regulation ends, or if there are a considerable amount of unregulated situations which makes the protection in some way inadequate in relation to the problem that HAO:s poses. Throughout this chapter, the essential aspects of the regulations of peacetime are discussed in regards to how they apply to cyber warfare and information influence operations—which are aimed at the attrition of the aggrieved State in question—or whether it lacks in its handling of HAO:s in some regards. This examination mainly includes general principles of peacetime regulation of international law, as well as those of State sovereignty, non-intervention and State responsibility.

3.1 The applicability of peacetime regulations to Hostile Attritional Operations

Before delving into the peacetime regulation pertinent to HAO:s, the obvious question which needs to be addressed is if the legal framework of peacetime in international law is at all applicable to HAO:s and—if so—how, why and when. The two constituents of HAO:s, cyber attacks and information influence operations, both share some common denominators which

[115] Bring et al., 2020, For a discussion of collective security versus peace and the possible inherent conflicts between these two concepts, see Wrange, 2015, pp. 104 f.f. Regarding cyberspace in this context, see also Delerue, 2020, p. 3.
[116] See e.g. the preamble and Chapter 1 of the UN Charter; Svanberg and Bring, 2019, p. 25. Regarding obligations to protect international peace, see also Chapters VI, VII and VIII of the UN Charter in tandem, Svanberg and Bring, 2019, pp. 25–26.
[117] See e.g. Fogt, 2020, p. 30 f.f.

makes the applicability of international law to the different forms of HAO:s suitable to discuss at one and the same time initially, even if they after this for the most part will be dealt with separately.[118] For starters, both cyber attacks and information influence operations are by and large occurring in or via cyberspace; it is, in this context, natural to ask if international law generally, and its peacetime regulations specifically, is applicable to cyberspace. The overall answer to this question is yes.[119] Having previously been the subject of controversy, for example, the United Nations Group of Governmental Experts have concluded that the UN Charter is applicable to cyberspace and information and communication technology (ICT).[120] Evidence of States having moved to or towards this position is also prevalent, with e.g. the then President of the United States, Barack Obama, in 2011 stating that

> "[t]he development of norms for cyberspace does not require an intervention of customary international law, nor does it render existing international norms obsolete. Long-standing international norms guiding state behavior – in times of peace and conflict – also apply in cyberspace. Nonetheless, unique attributes of networked technology require additional work to clarify how these norms apply and what additional understandings might be necessary to supplement them."[121]

Thus, notwithstanding the lack of cyber-specific custom, today, there has at least been an evolution in State practice and doctrine which accepts the general applicability of international law on activities, operations or other forms of conduct taking place in cyberspace. Therefore, the starting point for the continued handling of HAO:s in peacetime is this: general public international law is applicable to HAO:s taking place in cyberspace.[122] Cyberspace is also the starting point for where both cyber attacks and information influence operations take place.[123] In the following, a short background to the central and general peacetime regulation will be given, before examining the conditions for applying it to the special kind of nature coining HAO:s.

---

[118] Mainly due to differences in the nature of the two constituents, see (generally) the definitions in Chapter 2.
[119] See e.g. Delerue, 2020, section 1.1.1, pp. 6–7.
[120] Tsagourias, 2015, pp. 13–14.
[121] The White House, "International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World", May 2011 [https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf], accessed 2024-11-22.
[122] This conclusion is also made by e.g. Delerue, 2020, p. 1.
[123] See further in section 2.1.1.

3.2 Foundations of the peacetime regulation(s) – a short outline

Public international law is built upon a number of principles (some coining specific areas of international law, while others being more general in nature), a couple of which have already been dealt with in the introductory parts of the thesis. Principles like pacta sunt servanda, pacta tertiis, jus cogens, etcetera, are such central tenets that are essential in the understanding of international law and its influence on the relations between States. Furthermore, generally in international relations, there is also a presumption of *bona fide*, i.e. the good will of one another.[124] This is a result of public international law being largely built upon treaties and the principle of *pacta sunt servanda*, i.e. a presumption of that international agreements—just like other forms of agreements, in everyday relations—shall be kept.[125] Especially the principle of bona fide, i.e. the presumed good will of another, is of relevance for peacetime regulations pertinent to HAO:s.

When treaties are concerned, Article 31(1) of the Vienna Convention on the Law of Treaties (VCLT) settles down that "[a] treaty shall be interpreted in good faith in accordance with the ordinary meaning to be given to the terms of the treaty in their context and in the light of its object and purpose". Thus, bona fide can be claimed to mark all international relations and agreements. Notwithstanding this, according to general international law, States are not subjected to a certain *type* of means of dispute resolution, even if they are limited in their conduct by norms, rules and treaties, some just by being a part of the international community,[126] as well as the obligations according to State responsibility and ARSIWA.[127] For example, The Friendly Relations Declaration and the UN Charter demands of States to submit to peaceful dispute resolution.[128] This is coining the way in which States are able to take countermeasures in the form of self-help in the peacetime regulations, which will be further dissected below.

---

[124] Bring et al., 2020, p. 19.
[125] Bring et al., 2020, pp. 18–19; Crawford, 2019, p. 434.
[126] Regarding the obligations under the UN Charter, also e.g. the preamble and Chapter 1 of the UN Charter; Svanberg and Bring, 2019, p. 25. Notwithstanding this, in order to fully understand the full width of the obligations aiming towards international peace are settled down which the UN Charter imposes on its member States, one has to read the Chapter's VI, VII and VIII in tandem, see Svanberg and Bring, 2019, pp. 25–26. See also Svanberg and Bring, 2019, p. 67.
[127] See below section 3.4.
[128] See Article 2(4) of the UN Charter and UNGA Res. 2625 (XXV), *The Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States*, 24 October 1970; Delerue, 2020, p. 423. Regarding Article 2(4) of the UN Charter, see subsection to section 3.3 below.

3.3 State sovereignty, non-intervention and State responsibility

3.3.1 The concept of State sovereignty

A core element in the understanding of this and international law, is the concept of State sovereignty; sovereignty is the foundation which the entirety of the international community rests upon, and is inevitability associated with the concept of the State itself.[129] The intention of the concept of sovereignty can be said to aim (at least in part) towards providing a basis for relations within international law, a sort-of natural starting point for States' legal capacity and self-determination.[130] Being such a fundamental concept within international law, it is closely linked to the exercise of power over e.g. the territory of the State in question.[131] While there are no universally accepted legal definitions of the term *sovereignty*,[132] however, within public international law, its implications impact the international community as well as the national States. Within the international community, the sovereignty concept signifies independence and equity between States.[133]

It is important to note that a State's sovereignty does not permit the State in question to behave as it pleases; as Bring et al. phrases it, "[sovereignty] has to be exercised under the [international] laws".[134] Even though the continued existence of the sovereignty terminology is debated and criticized,[135] it is still essential to be familiar with the concept of sovereignty, since it is the basis for the application of public international law.[136] The meaning of sovereignty and question of its width, as well as its development in connection to the Friendly Relations Declaration, will be discussed and elaborated on in the preceding sections. The question of sovereignty in relation to the principle of non-intervention will in this context also be touched upon, in regards to the legal frameworks pertinent to HAO:s.

3.3.2 Non-intervention, non-interference and distinctions of other forms of breaches of public international law

A consequence of the prevalence of State sovereignty within international law, is the development of the principles of non-intervention within the legal area of international use of

[129] Bring et al., 2020, p. 73.
[130] Linderfalk et al., 2020, pp. 22–23.
[131] McCorquodale and Dixon, 2003, p. 234.
[132] Bring et al., 2020, p. 73.
[133] Bring et al., 2020, pp. 73–74; Delerue, 2020, pp. 233–234.
[134] Bring et al., 2020, p. 74 (translation by the author of the thesis).
[135] For further discussions on questions pertaining to State sovereignty, see e.g. Bring et al., 2020, pp. 22–26; Henriksen, 2017, p. 12.
[136] See Clapham, 2012, p. 46.

force.[137] In short, non-intervention means that one State is not allowed to interfere with the internal affairs of another State.[138] A general reference for its definition can be made to the Nicaragua case, where the principle of non-intervention is referred to as "the principle [which] forbids all States or groups of States to intervene directly or indirectly in internal or external affairs of other States."[139] Furthermore, also emerging from the principle of non-intervention, the principle of non-interference instead refers to the prohibition of "interference by a State in the internal or foreign affairs of another State."[140]

From the non-intervention principle flows the prohibition of use of force. This is enshrined in Article 2(4) and 2(7) in the UN Charter,[141] where in the former it is stated that it is prohibited to either threaten with violence or exercise violence as a method to the means for a State to achieve its goals.[142] While discussing non-intervention, it is important to be in the clear about the terminology regarding the term use of force, and concepts pertinent to it. The terms use of force and intervention are two different but overlapping terms, with *use of force* referring only to such *military* violence that is a violation of the UN Charter.[143] Therefore, when using the term to *use of force*, it is not a question of such (even though it can be perceived as a "punishment" by an affected State) if it only consists of political or economical measures, like economic sanctions that are aimed at strike against a State as a response to i.e. an aggression, or other such behavior affects the international community in some way.[144]

Furthermore, there are even narrower concepts within this area of international law, that by design are not applicable to HAO:s. Examples are the terms armed attack and aggression, with the latter being the most serious breach that a State can be considered to commit against another. Aggression constitutes, according to a UN Resolution,

> "[t]he use of force by a State against the sovereignty, territorial integrity or political independence of another State, or in any other manner inconsistent with the Charter of the United Nations, as set out in this definition."[145]

---

[137] Crawford, 2019, p. 431.
[138] Bring et al., 2020, p. 185.
[139] *Military and Paramilitary Activities in and against Nicaragua* (Nicaragua v. United States of America) (Judgement) (Merits), ICJ Reports 392, p. 106, para 202.
[140] Delerue, 2020, p. 232.
[141] Bring et al., 2020, p. 185.
[142] There are two exceptions from the prohibition of the use of force; first, collective or individual self-defense warrants such use of force that is acceptable under the UN Charter; second, measures that are sanctioned by UN:s Safety Council are considered to be such an exception from the prohibition of use of force, see Bring et al., 2020, p. 192.
[143] Bring et al., 2020, p. 185.
[144] Bring et al., 2020, p. 185. See instead i.e. Article 48 and 54 in ARSIWA.
[145] See the definition in UNGA Resolution 3314 (XXIX), Article 1.

While this not being entirely clear in regards to what *kind* of force is intended, when it concerns the definition of use of force, in Article 3 of the same resolution, the meaning of aggression is expressed; i.e. invasion or attack by the armed forces of a State against another,[146] bombardment of one State against another State's territory,[147] inter alia. However it may be, these requirements clearly state that it is some form of violence that is intended. What can be concluded from this, is that HAO:s—or hybrid warfare in the form of cyber attacks and information influence operations—cannot *prima facie* amount to such use of force that is intended with violence or use of force, according to the UN Charter.

Notwithstanding this, there are still other breaches a State can commit, even though it does not amount to violence as the term use of force sets forth. Returning to the question of non-intervention, here, one has to be familiar with the term *intervention*; the definition does not necessarily demand that use of force has been committed. Intervention, and the prohibition of it—i.e. the principle of non-intervention—can therefore refer to other means than military violence or use of force.[148] What is to be considered a breach from the non-intervention principle emerges from the Friendly Relations Declaration, where it is stated that

> "[n]o State or group of States has the right to intervene, directly or indirectly for any reason whatsoever, in the internal or external affairs of any other State. Consequently, armed intervention and all other forms of interference or attempted threats against the personality of the State or against its political, economic and cultural elements, are in violation of international law.
>
> No State may use or encourage the use of economic, political or any other type of measures to coerce another State in order to obtain from it the subordination of the exercise of its sovereign rights and to secure from it advantages of any kind. Also, no State shall organize, assist, foment, finance, incite or tolerate subversive, terrorist or armed activities directed towards the violent overthrow of the regime of another State, or interfere in civil strife in another State.
>
> The use of force to deprive people of their national identity constitutes a violation of their inalienable rights and of the principle of non-intervention.
>
> Every State has an inalienable right to choose its political, economic, social and cultural systems, without interference in any form by another State".[149]

[146] UNGA Resolution 3314 (XXIX), Article 3(a).
[147] UNGA Resolution 3314 (XXIX), Article 3(d).
[148] Bring et al., 2020, p. 185.
[149] UNGA Resolution 2625 (XXV), *The Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States*, 24 October 1970.

Clearly, the Friendly Relations Declaration sets forth a wider definition than the more narrow definition of what is considered an intervention according to the UN Charter, i.e. by demanding that the use of force have occurred. When navigating the peacetime regulations and the principle of non-intervention, it is the lower threshold reflected in the Friendly Relations Declaration that one has to relate to. Furthermore, coercion is a central aspect of the principle of non-intervention, especially for this thesis (and information influence operations), where ICJ:s wording of the prohibition of "methods of coercion in regard to such choices, which must remain free ones"[150] will be returned to in the following sections.

3.4 State responsibility and Internationally Wrongful Acts By a State

In order to function properly, for the international community, it is of necessity that States are being held responsible when they commit breaches of their obligations.[151] State responsibility is a so-called secondary obligation within international law,[152] in contrast to the primary rules that regulates what States do,[153] and is often referred to as *violation of international law* (or *internationally wrongful act*).[154] State responsibility is generally considered to be customary international law, although reflected in the ILC:s Articles on State Responsibility (ARSIWA). Thus, it is not a question of a behavior which qualifies as a criminal ditto or an act of war, but rather constitutes such obligations which States shoulders in relation to one another, bearing the mark of being a civil matter.[155] In other words, States have a primary responsibility to abstain from breaking its obligations, and a secondary obligation to repair the damage caused (Article 30, 34–39 of ARSIWA).[156] State responsibility's secondary nature can thus be described as referring to the legal area dealing with the consequences of a State's (internationally) wrongful act; how it is being dealt with is dependent on what kind of breach it is that has been committed.[157] In this context, peacetime reprisals—which nowadays are referred to as countermeasures—are also discussed.

The general principle of internationally wrongful acts is enshrined in Article 1 of ARSIWA, where it is stated that "[e]very internationally wrongful act of a State entails the

[150] *Military and Paramilitary Activities in and against Nicaragua* (Nicaragua v. United States of America) (Merits), ICJ Reports 14, 1986, para 205.
[151] Henriksen, 2017, p. 127.
[152] Bring et al., 2020, p. 146.
[153] Henriksen, 2017, pp. 127–128.
[154] Bring et al., 2020, p. 146.
[155] See Bring et al., 2020, p. 146.
[156] Bring et al., 2020, p. 154.
[157] See Crawford, 2002, pp. 196–200; Bring et al., 2020, pp. 154–155.

international responsibility of that State".[158] An international wrongful act, in turn, consists of two elements: 1) an action or omission attributable to a State, which 2) constitutes a breach of an international obligation (Article 2 of ARSIWA).[159] The examination in regards to the respective HAO constituent will be analysed in the light of the latter criterion, as questions pertaining to attribution falls outside the scope of this thesis.[160] Moreover, the characterization of a wrongful act is dependent on what is considered unlawful according to *international* law (Article 3 of ARSIWA).[161] This means that one has to examine primary obligations of international law in order to determine what is prohibited according to international law, which is the aim of the following sections, especially pertaining to the HAO constituents and the assessment of countermeasures available to victim States.[162]

Below, first, the respective constituent of HAO:s will be assessed and discussed in regards to their law- or unlawfulness according to the ARSIWA; second, this lawfulness or unlawfulness will be analyzed in regards to retorsion and other forms of countermeasures which States are allowed to take in accordance with international law. In this context, and as will be apparent, much like when operating in armed conflict,[163] States have to relate to e.g. the principle of proportionality in the taking of countermeasures.

3.5 Applying the peacetime framework on Hostile Attritional Operations

Since the approach in this thesis to a large degree is explorative, the navigation here before has initially been based on the assumption of international law being applicable to HAO:s, which is supported by the literature on the subject matter.[164] This specific section aims at examining the handling of the HAO constituents, i.e. the application of the peacetime regulations on cyber attacks and information influence operations. Building on the background to general international law, which has been given in the preceding section, the identified regulations and legal aspects of relevance will be applied on the HAO constituents. At length, the aim is to examine whether HAO:s are regulated or prohibited in the peacetime regulations and—if so—to what extent, the above mentioned aspects of peacetime

[158] See further Crawford, 2002, pp. 77–80.
[159] See further Delerue, 2020, p. 242; Crawford, 2002, pp. 81–85.
[160] See further in section 1.2.
[161] Crawford, 2002, pp. 86–90.
[162] See section 3.8.
[163] See e.g. section 4.2.3.
[164] The International Group of Experts of the Tallinn Manual 2.0 are, for instance, of this opinion.

international law will be further elaborated on in relation to the respective constituent, beginning with cyber attacks and continuing on to information influence operations.

3.6 Cyber operations (attacks) in peacetime

Notwithstanding the very real concern of at all being able to attribute a certain unlawful conduct to a State or State actor, one has to be able to imagine a scenario where practical problems like attribution are solved, in order to map out solutions for such situations. A first point of departure is that cyber attacks are—without a doubt—of the character that indeed cause damage to a State's interest. Once a cyber operation can be attributed to a certain State, it renders the question whether it constitutes an internationally wrongful act which amounts to an act which triggers the regulation of State responsibility, and thus being possible to counter by leaning on its rules.

In the following, the approach begins once the cyber attack in question has been attributed to a State or State actor, and the main question which is aimed at being answered is in what way cyber attacks can be considered a breach of State sovereignty, non-intervention and an unlawful operation governed by ARSIWA. I.e., does cyber attacks or operations constitute a breach of international norms in peacetime? A starting point in this examination is that there is a lack of a general prohibition of cyber operations, nor does it *per se* constitute such a breach of international law that is considered unlawful.[165] For example, it is settled in ICJ:s Nicaragua case that unfriendly acts are not automatically prohibited by international law.[166] As has been mentioned in the above, however, both the UN Charter and the Friendly Relations Declaration sets forth that States "shall" refrain from non-peaceful resolutions of conflicts.[167] Unfortunately, if one is looking for more strict obligations which can be breached if the State in question does not follow this exhortation, neither the UN Charter nor the Friendly Relations Declaration provide such.[168]

Another starting point for the continued exploratory navigation of the handling of cyber attacks or operations in peacetime, which is set out in the Lotus case from ICJ:s

---

[165] Delerue, 2020, pp. 193–194; Tallinn Manual 2.0, Chapter 5, "Cyber operations not *per se* regulated by international law", p. 168.
[166] *Military and Paramilitary Activities in and against Nicaragua* (Nicaragua v. United States of America) (Merits) [1986], ICJ Reports 14, pp. 136–137, para 273.
[167] See e.g. *Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in Accordance with the Charter of the United Nations*, Res. 2625 (XXV) (24 October 1970), p. 103.
[168] Delerue, 2020, p. 195.

predecessor PCIJ, is the tenet of "what is not prohibited is permitted" in international law.[169] However criticized this outcome might have been,[170] the presumption is that the opposite would limit States in a way which stands in conflict with State sovereignty and—as will be apparent in the following sections—cyber operations can in fact be considered as violations of State sovereignty, as well as a possible breach of the principle of non-intervention.

3.6.1 Cyber attacks as a breach of (State) sovereignty

As has previously been ascertained, the concept of sovereignty is central to international law in both peacetime and armed conflict,[171] and it is clear from its sources that the existence of (State) sovereignty is something that States have to take into account; cyberspace is no exception to which sovereignty does not apply.[172] The starting point when navigating the regulation of cyber attacks (or operations) is that State sovereignty is applicable to conduct which takes place in cyberspace, at least according to the expert group behind the Tallinn Manual (2.0). The principle of sovereignty is no exception.[173] The definition of sovereignty, which is used in the Manual, is based on that which was established in the Island of Palmas arbitral award (1928), namely "[s]overeignty in the relations between States signifies independence. Independence in regard to a portion of the globe is the right to exercise therein, to the exclusion of any other State, the functions of a State".[174] This is the same definition which is leaned on in regards to cyberspace activities in this thesis, not only because it enjoys wide recognition, but because it is helpful in understanding the aspects of sovereignty which makes cyber operations worth considering as a possible violation of State sovereignty, when it is conducted in cyberspace.

The question of whether sovereignty is applicable to "the web" (or *in cyberspace*) has, however, not always been clear.[175] First off, there are concerns emerging from the fact that cyberspace *prima facie* is not tied to any specific territory, which State sovereignty is

[169] See *S.S. "Lotus"* (France v. Turkey), Judgment, Judgment No 9, PCIJ Series A No 10, ICGJ 248 (PCIJ 1927), (1935) 2 Hudson, World Ct Rep 20, 7th September 1927, League of Nations (historical) [LoN]; Permanent Court of International Justice (historical) [PCIJ].
[170]The "Lotus Dictum" has been criticized by Judge Simma in *Accordance with international law of the unilateral declaration of independence in respect of Kosovo*, Advisory opinion, ICGJ 423 (ICJ 2010), 22nd July 2010, International Court of Justice (ICJ).
[171] Tallinn Manual 2.0, 2017, "Rule 1 – Sovereignty (general principles)", para 1.
[172] Tallinn Manual 2.0, 2017, "Rule 1 – Sovereignty (general principle)".
[173] Tallinn Manual 2.0, 2017, "Rule 1 – Sovereignty (general principle)".
[174] *The Island of Palmas Case*. Permanent Court of Arbitration, 1928.
[175] Delerue, 2020, p. 1 f.f.

concerned with in regards to the State's competence over its own territory.[176] As Delerue puts it, cyberspace is in fact a "fictional territory".[177] However, when the experts of the Tallinn Manual settle down lex lata pertinent to sovereignty a State has the right to both internal and external sovereignty, this is considered to apply to cyber activities as well.[178] In Rule 2 of the Tallinn Manual, for example, the experts expresses that "[a] State enjoys sovereign authority with regard to the cyber infrastructure, persons, and cyber activities located within its territory, subject to its international legal obligations", i.e. referring to internal sovereignty, clarifying it in the commentary as "[…] a State is free to adopt any measure it considers necessary or appropriate with regard to cyber infrastructure, persons engaged in cyber activities, or cyber activities within its territory".[179] Rule 3, instead, settles down lex lata pertaining to external sovereignty, where it is stated that States are free to conduct cyber activities in its international relations, as long as there is not any prohibition of it which finds its source in international law.

Conclusively, and perhaps most importantly, the authors of the Tallinn Manual sets forth that "[a] State must not conduct cyber operations that violate the sovereignty of another State", and elaborates in the commentary that cyber operations which hinders a State from exercising its sovereignty is prohibited by international law.[180] Thus, a cyber operation which infringes upon this right to exercise sovereignty is to be viewed as a sovereignty violation, no less than comparable operations or activities which do not take place in cyberspace. The assumption in the following section is therefore that States are obligated to respect the sovereignty of one another, also in cyberspace and during peacetime.[181]

3.6.2 Cyber attacks and non-intervention

The principle of non-intervention—in an international law context, legally rooted in Article 2 of the UN Charter—lets us know that States are prohibited from violating the territory of another State, and has (as mentioned in previous sections) ties to the principle of State

[176] Crawford, 2019, p. 431; Delerue, 2020, p. 203. However, it is important to note that jurisdiction and sovereignty are principally two distinct concepts, see e.g. Delerue, 2020, p. 208 f.f.
[177] Delerue, 2020, p. 206.
[178] See the Tallinn Manual 2.0, 2017, "Rule 1 – Sovereignty (general principle)", "Rule 2 – Internal sovereignty" and "Rule 3 – External sovereignty" in tandem.
[179] Tallinn Manual, Rule 2, para 1, where it also is clear that this carries the condition of not violating e.g. human rights obligations, see Rule 35 of the Manual.
[180] Tallinn Manual 2.0, Rule 4, para 1.
[181] For an elaboration on violation of State sovereignty when the conduct is attributable to e.g. a corporation in Tallinn Manual 2.0, Rule 5, para 2.

sovereignty.[182] The meaning of the principle of non-intervention, having been settled in ICJ:s Nicaragua case, is to prohibit States, individually or collectively, to intervene "directly or indirectly" in "internal or external affairs of other States".[183] So, how does the principle of non-intervention apply to cyber attacks? Delerue calls this "cyber intervention" and relies on three elements when determining what is considered an "unlawful" intervention by using cyber; it has to be a question of 1) an act conducted by a *State* directed at another, which 2) is conducted with the intent of coercing the aggrieved State, and 3) this aggrieved State's to freely decide.[184] The Tallinn Manual 2.0, on the other hand, makes the distinction between sovereignty and non-intervention by leaning on the element of intervention "[…] requires an element of coercion".[185]

As Delerue shows, cyber operations (or attacks) can be useful for States in order to coerce others, an assumption which can be argued for by leaning on the experiences pertaining cyber activities, attacks and operations from the last two decades.[186] For example, the cyber operation which was suspected to have been conducted by Russia against Estonia in 2007 was such an unlawful intervention according to these criterias, mainly due to the fact that it had been conducted with the intent to "interfere with the internal affairs of another".[187] Attribution problems aside, what one needs to take note of when assessing these situations is that it is the *coercing* of an aggrieved State in combination with the *intent* to interfere with the internal affairs of said State. This is also the case concerning information influence operations, which will be apparent below.

3.6.3 State responsibility and breaches of primary responsibilities by cyber attacks

As has been ascertained above, State responsibility demands of States to primarily avoid certain conduct, and secondarily lays upon them an obligation to repair the damage done (Article 30 and 34–39 ARSIWA).[188] The Tallinn Manual 2.0 has settled the lex lata and State responsibility on questions pertaining to cyberspace and State Responsibility, which can be

[182] Delerue, 2020, pp. 232–233.
[183] *Nicaragua Case*, p. 106, para 205.
[184] Delerue, 2020, p. 239.
[185] Wheatley, 2020, p. 165; Tallinn Manual 2.0, 2017, Rule 66.
[186] See the examples of Sony Pictures, Stuxnet and Estonia in Delerue, 2020, pp. 239–241.
[187] Delerue, 2020, p. 241.
[188] See also e.g. the rule regarding Tallinn Manual 2.0, 2017, Rule 28, para 1 with reference to *Factory at Chorzow*, Judgement (Merits), PCIJ, 13 September 1928, at 47; Bring et al., 2020, pp. 154–155; Crawford, 2002, pp. 196–200 (Article 30); pp. 211–241 (Article 34–39).

found in Chapter 4 of the Manual.[189] While the Experts recognises that some of the content of the ARSIWA are not (yet) settled international law,[190] the customary law which is reflected in ILC:s ARSIWA (and constitutes more indisputable international law) is "undeniably" considered to be applicable to cyber operations.[191]

Having ascertained and accepted this observation as lex lata for the current examination, the necessary next step is to consult the Tallinn Manual 2.0 on in what way these breaches of State sovereignty and non-intervention can constitute an internationally wrongful act which generates State responsibility according to ARSIWA. In Rule 14 of the Tallinn Manual 2.0, it is settled that States bear international responsibility for cyber-related acts which 1) are attributable to a State, and 2) breaches international legal obligations.[192] The possible breaches of sovereignty and non-intervention by cyber operations has already been discussed in the above. The question here is what the consequences are, when both of these criterions have been confirmed to be present. The general principle of State countermeasures are reflected in Rule 20 of the Tallinn Manual 2.0, where it is stated that States may be entitled to take countermeasures in response to a breach of an international legal obligation, regardless of whether the breach was conducted in cyberspace or not. An example of what can be a target of a countermeasure, in response to a breach of international law conducted in cyberspace, is the cyber infrastructure of the State responsible for the breach of the obligation, which it has according to international law.[193] Once the responsible State has been engaging in an internationally wrongful act, the countermeasure which the aggrieved State conducts in response to the wrongful act is lawful (within limits, see below).[194] It is important to stress that the States which are entitled to take countermeasures are those that have been injured as a result of the internationally wrongful act.[195]

However, according to Rule 21 of the Tallinn Manual, the purpose of the countermeasure in question has to be limited to make the responsible State comply with the legal obligation it has in relation to the aggrieved State.[196] Here, it is emphasized that e.g. the risk of escalation needs to be taken into account when conducting the countermeasure.[197]

---

[189] Tallinn Manual 2.0, 2017, "4. Law of international responsibility".
[190] Tallinn Manual 2.0, 2017, "Section 1: Internationally Wrongful Acts By A State", para 1.
[191] Tallinn Manual 2.0, 2017, "Section 1: Internationally Wrongful Acts By A State", para 4.
[192] Tallinn Manual 2.0, 2017, Rule 14. While attribution—with regards to the scope of the thesis—is not elaborated on to any further extent here, it is still a necessary element of State responsibility both in theory and in practice, see Tallinn Manual, 2.0, 2017, Rule 15–17; Rule 20, para 7. See also Delerue, 2020, Chapter 4.
[193] Tallinn Manual 2.0, 2017, Rule 20, para 6.
[194] Tallinn Manual 2.0, 2017, Rule 20, para 6.
[195] Tallinn Manual 2.0, 2017, Rule 24.
[196] Tallinn Manual 2.0, 2017, Rule 21, para 2.
[197] Tallinn Manual 2.0, 2017, Rule 21, para 2.

Furthermore, countermeasures are associated with limitations, which is further specified in Rule 22; the aggrieved State is *not* allowed to violate fundamental human rights, jus cogens rules or conduct such countermeasures which amounts to "belligerent reprisals" which are prohibited by international law.[198] Aggrieved States are also limited by proportionality in its conduct of countermeasures, which the group of Experts clarify in the commentary to Rule 23, where it also reiterates that the Rule in question is reflective of Article 51 of ARSIWA.[199]

3.7 Information influence operations in peacetime

The legality of the spreading of propaganda during peacetime is, much like cyber attacks, dependent on whether the information influence operation in question can be considered a breach of State sovereignty, a breach of the principle of non-intervention or an internationationally wrongful operation which is governed by the State responsibility. Since the kinds of information influence operations which the thesis has been limited to is presumed to have been conducted on the internet, the examination of information influence operations in peacetime regards the same elements as has been discussed in the above; i.e. breaches of sovereignty, non-intervention and issues pertaining to State responsibility and information influence operations.

Similarly to the handling of cyber attacks, the Tallinn Manual can be of use when deciphering lex lata and the handling of information influence operations which have been conducted on the internet. In this context, the rules which regulate cyberspace are of relevance, and have already been dealt with to some extent in the above. Here, some other doctrinal sources will be relied on to interpret international law, as well as give perspective on possible angles of incidence pertaining to the occurrence of information influence operations in peacetime.

3.7.1 Information influence operations, sovereignty and non-intervention

While propaganda has been used by States for centuries by spreading information in a physical form, information influence operations are, in today's highly technologized society, often conducted on the internet. Non-intervention in a cyber context has already been dealt

[198] Tallinn Manual 2.0, 2017, Rule 22. Regarding the prohibition of violating fundamental human rights is a reflection of Article 50(1) of ARSIWA, see Tallinn Manual 2.0, 2017, Rule 22, para 3. Regarding peremptory norms of general international law in Article 53 of the Vienna Convention, see Tallinn Manual 2.0, 2017, Rule 22, para 6 f.f.
[199] Tallinn Manual 2.0, 2017, Rule 23, para 1. See also Tallinn Manual 2.0, 2017, Rule 26 regarding necessity.

with in regards to cyber *attacks* or *operations* in the above, but as has also been ascertained, information influence operations often have different consequences, being more long-term and abstract in nature; in fact, influence operations are perceived to possibly constitute a violation of the principle of non-intervention.[200] Furthermore, information influence operation can be argued to contain an element of *coercion* that is distinctive for this type of HAO. Influence operations, when conducted in cyberspace, have been referred to as "a new form of State propaganda".[201] As Wheatley (2020) puts it, "the Internet" (here referred to as cyberspace) has made it possible for foreign States to influence individuals and the on-going political discussions in another State.[202]

Wheatley further argues that it is the coercion element which is of interest in this context; while providing the citizenry in another State with information based on facts is *not* considered unlawful under international law, such information influence that classify as subversive propaganda *is*.[203] By dwelling on the question of whether an information campaign can be considered "coercive", Wheatley acknowledges that the strict "providing of facts" is not considered unlawful, however, the exception to this is when the foreign State, by pushing a single political narrative "drowns out" the opposition, which he—in contrast—argues would constitute unlawful conduct.[204]

Delerue (2020) has instead treated influence operations as a *part* of a (presumed larger) influence operation.[205] The most prevalent example when it comes to information influence operations in peacetime—which Delerue also partly relies upon—is perhaps the 2016 US presidential election, which was in fact an attempt to influence the democratic process in the aggrieved victim State in question.[206] According to Delerue, the conduct which consisted of one or more *separate* cyber incidents—in and of oneself or separately—did *not* amount to an unlawful intervention, but rather constituted a breach of State sovereignty.[207] However, together with the other conduct which constituted a larger *influence* operation, this would, according to Delerue, be a breach of non-intervention.[208] As Delerue regards cyber

[200] Wheatley words it as "foreign intervention" (in elections), which is here considered to be *a form of* information influence operation, see Wheatley, 2020, p. 162.
[201] Wheatley, 2020, p. 187.
[202] Wheatley, 2020, p. 187.
[203] Wheatley, 2020, p. 187, f.n. 153 with references; p. 189.
[204] Wheatley, 2020, p. 189.
[205] Delerue, 2020, section 5.4.2.2.
[206] Delerue discusses this in terms of "the election process", while the stance in this thesis is that information influence operations have broader implications and constitutes such conduct which have consequences that are more long-term in nature, i.e. threats to democracy at large.
[207] Regarding the criterions for an unlawful intervention in cyberspace, see section 3.6.2 and Delerue, 2020, p. 239.
[208] Delerue, 2020, pp. 241–242.

attacks as a means with which a cyber attack can be carried out, the emphasis is instead put on whether cyber attack can be categorized as a preparatory or composite act, which is necessary to determine in order to further examine the State responsibility according to ARSIWA.

3.7.2 Information influence operations as Internationally Wrongful Acts by a State

If an information influence operation is conducted in cyberspace and can be considered a breach of an international obligation, the responses available to the information influence operation in question are based on the same articles of ARSIWA that concerns cyber operations, which has already been outlined and described in section 3.6.3 above. However, since information influence operations according to some scholars are viewed as a composite act, this renders an additional approach in some regards. Article 15(1) of ARSIWA codifies breaches of an international obligation by a State, which "through a series of actions or omissions defined in aggregate as wrongful occurs when the action or omission occurs which, taken with the other actions or omissions, is sufficient to constitute the wrongful act". The significant element of these kinds of breaches is specified in Article 15(2), where it is said that "[…] the breach extends over the entire period starting with the first of the actions or omissions of the series and lasts for as long as these actions or omissions are repeated and remain not in conformity with the international obligation".

Thus, information influence operations—when viewed from this angle—could be argued to be counterable in accordance with Article 15 ARSIWA, by leaning on the ability to break down the influence operation to its different ingredients, and thus tackle them "one by one". However, if the act in and of itself is to be categorized as a *preparatory* action which, in turn, is *not* categorized as an internationally wrongful act, this falls outside the scope of application.[209] The distinction between composite and preparatory acts—the former being unlawful while the latter are considered lawful—has been made dependent on whether the actions in question "[do] not […] predetermine the final decision to be taken".[210] This was established by ICJ in the Gabčíkovo-Nagymaros Project case, where it was stated that "[a] wrongful act or offence is preceded by preparatory actions which are not to be confused with the act or offence itself. It is as well as to distinguish between the actual commission of a wrongful act […] and the conduct prior to that act which is of a preparatory character and

[209] Delerue, 2020, p. 243.
[210] Commentary to the Articles on State Responsibility, pp. 61–62; Delerue, 2020, p. 243.

which 'does not qualify as a wrongful act […]'".[211] The fact that preparatory actions prima facie are considered to be lawful has implications for the legality of HAO:s, since the perceived problem with the phenomena in question is that they *are* preparatory in nature, an issue which will be further addressed in the following.

3.8 Obligations, self-help and countermeasures

3.8.1 Obligations according to Articles on State Responsibility

There are several consequences for a responsible State, having committed a violation or breach of international law. First, the responsible State engaging in a continuing internationally wrongful act has an "obligation to cease" (Article 30[a] of ARSIWA).[212] According to Delerue, various forms of cyber operations are of the character that they are "continuing" in nature and, if so, the responsible State perpetrating the cyber operation has an obligation to cease its conduct.[213] Second, the responsible State also has an obligation to offer assurances and guarantees of non-repetition (Article 30[b] of the ARSIWA).[214] Third, there is an obligation of making reparation (Article 31 of the ARSIWA).[215] Delerue has elaborated on the notion of injury in regards to cyber operations, which according to Delerue has suffered a debate that has been preoccupied with the semantic meaning of the notion.[216] According to the ILC and Article 31(2) of ARSIWA, it concerns injury regardless of it being "material or moral". However, all this is dependent on whether the activity or conduct, in this case in the form of a HAO, constitutes a breach or violation of international law, i.e. an "internationally wrongful act", the challenges of which have already been discussed to some degree in the above. One question which emerges here is if the conduct is to be categorized as a retorsion or international wrongful act to which countermeasures, as a response, are allowed.

3.8.2 Perspectives on retorsion

Varying kinds of countermeasures are also a possibility for a State exposed to internationally wrongful acts; sometimes, even if there has not been a formal internationally wrongful act. In the peacetime regulation, these are called "measures of self-help", a sort-of recourse to

[211] *Gabčíkovo-Nagymaros Project* (Hungary v. Slovakia) (Judgement), 1997, ICJ Reports 88, p. 54, para 79.
[212] Regarding cessation, generally, see Delerue, 2020, pp. 382–388 (section 9.1 and subsections).
[213] Delerue, 2020, section 9.1.3, p. 388.
[214] Delerue, 2020, pp. 388–392. See also *LaGrand* case (Germany v. United States), ICJ Reports 466, 2001, pp. 514–516, paras 127 and 128(6).
[215] *Factory at Chorzów* (Merits) (Judgement), PCIJ Series A No 17, 8 February 1927/13 September 19, Permanent Court of International Justice [PCIJ], p. 21.
[216] Delerue, 2020, p. 394.

"extrajudicial measures" in order to impose on the responsible State to comply with its obligation according to international law.[217] According to Delerue, States' right to self-help is scarcely dealt with in literature, in contrast to the question of self-defence which is more focused on.[218] Moreover, Delerue is of the opinion that most cyber operations do not amount to an attack in the LOAC sense of things, which is why self-defence often is out of consideration in most cases.[219] That leaves us with the following measures available for a victim State in peacetime: retorsion and (some forms of) countermeasures.

Retorsions are, according to Delerue, "lawful but unfriendly".[220] However, as has previously been discussed, unfriendly acts are not *per se* prohibited by international law; one of the few restrictions which are put upon them are that they are submitted to be conducted in accordance with international law.[221] Retorsion is characterized by being a lawful response to e.g. a malicious State having been responsible for injurious activities.[222] While restrained by the demand of the retorsion in question having to be lawful, the responding States are unlimited in the choice of *how* and *when* to conduct it.[223] Moreover, Delerue sets forth that the conduct of retorsion is a political question more than it is a legal ditto, and the use of which lets the State in question express disagreement with the opposing State's activities.[224] The General Assembly has expressed condemnation with certain forms of retorsion,[225] making the use of which is controversial in some aspects. Furthermore, it is recognized that cyberspace can constitute a useful tool for conducting retorsion.[226] It is important to note, however, that retorsion goes "both ways"; the cyber operations conducted against Estonia in 2007 (and against Georgia in 2008, both allegedly conducted by Russia), for example, are believed to be in response to "disagreeable behavior" conducted by the victim State Estonia, which consisted of removing a Soviet statue.[227]

---

[217] Delerue, 2020, p. 423. Countermeasures are considered "the main extrajudicial and decentralised mechanism for securing compliance with international law", see Delerue, 2020, p. 434. See also Crawford, 2013, p. 676.
[218] Delerue, 2020, p. 423.
[219] Delerue, 2020, p. 424.
[220] Delerue characterizes them as "unfriendly, discourteous, rigorous, unfair, inequitable or prejudicial", Delerue, 2020, p. 424. Regarding retorsion, generally, Delerue, 2020, section 10.1 with subsections.
[221] Delerue, 2020, p. 425.
[222] Retorsion can also be used to "counter" (or show displeasement with) perfectly lawful conduct, see Delerue, 2020, p. 425.
[223] Delerue, 2020, p. 425. If a State responds to an internationally wrongful act, however, it is not limited by it having to relate to the threshold of legality, see Delerue, 2020, pp. 425–426.
[224] Delerue, 2020, pp. 425–426.
[225] See e.g. UNGA Resolution 2131 (XX), *Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their Independence and Sovereignty*, 21 December 1965.
[226] Delerue, 2020, p. 426.
[227] Delerue, 2020, pp. 427–428.

Setting the attribution question aside, Delerue argues that the lawfulness of the operations need to be assessed as two different forms of (influence) operations as responses which could either be categorized as retorsion or a breach of international law, namely the principle of non-intervention.[228] Like Wheatley (2020), Delerue takes hold of the coercion aspect of the principle of non-intervention when determining whether it is a question of retorsion or unlawful conduct, i.e. a breach of international law.[229] The conduct which Russia allegedly was responsible for, would in Delerue's opinion most likely constitute a lawful retorsion when assessed in isolation. However, when assessing them as composite parts of a larger operation, and when adding an unlawful *objective* to the equation, it could be argued to consist of a breach of the non-intervention principle.[230] When reviewing the State practice on measures of retorsion, nonetheless, it shows that States have not (yet) moved towards categorizing such cyber operations as internationally wrongful acts.[231]

3.8.3 Countermeasures and proportionality in a cyber (peacetime) context

As has been concluded before in the above sections, other forms of countermeasures[232]—on the other hand—are available for a victim State when a prior internationally wrongful act has been conducted by another, responsible State.[233] Notwithstanding the above conclusion on States apparently having been reluctant on moving towards viewing the varying forms of cyber operations as internationally wrongful acts; if one were to imagine a situation in which they were to, this could warrant the victim State the ability to take countermeasures against the responsible State. Rules on countermeasures are enshrined in the ARSIWA,[234] and has been analysed by e.g. Delerue in the light of cyber activities, where it is set forth that countermeasures are "multifunctional" in nature, and impacts the proportionality assessment of the countermeasure in question.[235] These functions can be summed up as countermeasures having 1) a normative function, 2) a retributive function, 3) coercive function, and 4)

[228] Delerue, 2020, pp. 427–428.
[229] Delerue, 2020, p. 428.
[230] Regarding the differentiation between lawfulness of *measures* and lawfulness of *objectives*, see Delerue, 2020, p. 428. See also the discussion on composite acts in the light of Article 15 of ARSIWA in section 3.7.2.
[231] Delerue, 2020, p. 431. See also the example of the U.S. responses to the DNC hack of 2016, Delerue, 2020, p. 431.
[232] These are to be distinguished from retorsion, Delerue, 2020, p. 436.
[233] Delerue, 2020, p. 438.
[234] See Articles 22 and 49–54 of the ARSIWA.
[235] Delerue, 2020, p. 436.

executive function.[236] For this specific thesis, it is perhaps the normative and executive functions which are of most apparent relevance.

Moving on to some of the frames and some limitations for taking countermeasures: first, countermeasures are only available to States which have been victim to an internationally wrongful act of another, responsible State (Article 49 of ARSIWA).[237] This "victim assessment" is made by the State exposed to the internationally wrongful act in question.[238] Second, it is not permissible to take "preventative" countermeasures.[239] Third, the countermeasure has to be aimed at the responsible State.[240] Fourth, the countermeasure taken should be reversible.[241] Moreover, the objective of the countermeasure in question is thought to make the responsible State comply with its international obligations; thus, it does not constitute a retaliation measure as such.[242]

It is important to note that the taking of countermeasures is submitted to the principles of proportionality and necessity are limited by certain "substantive conditions".[243] One of these principles is necessity, which demands of the State to take such countermeasures which are *necessary* in order to make the responsible State act in accordance with its obligations under international law.[244] The other main one being proportionality, in turn compelling the victim State to assess the expected outcome with "ration and reason", in order for the countermeasure in question to be valid.[245] These principles are also reflected and confirmed in the Tallinn Manual 2.0, regarding its implication for cyber-related operations.[246]

3.9 Conclusion: Hostile Attritional Operations in peacetime

The point of departure in this Chapter was to examine if, and—if so—in what ways and to what extent HAO:s in the form of cyber attacks and information influence operations can violate rules and stipulations in the peacetime regulation of public international law. With this as a guiding star for the navigation in the peacetime regulation, aspects which have been of

---

[236] Delerue, 2020, p. 436.
[237] Generally, see Delerue, 2020, section 10.2.1.1 "Unilateral Measures"; 10.2.1.2 "Prior Wrongful Act" (latter reference regards p. 438 f.f.).
[238] Delerue, 2020, pp. 437–438.
[239] Delerue, 2020, p. 438.
[240] Delerue, 2020, p. 439.
[241] This is not an "absolute condition" for taking the countermeasure in question, see Delerue, 2020, p. 440.
[242] Delerue, 2020, p. 441.
[243] Delerue, 2020, section 10.2.3 "Substantive Conditions", pp. 448 f.f.
[244] Delerue, 2020, p. 448.
[245] The principle of proportionality also has implications for jus in bello or Law of Armed Conflict (LOAC), which will be apparent in Chapter 4 below. See also e.g. Delerue, 2020, p. 448.
[246] Generally, see Tallinn Manual 2.0, 2017, "[Chapter] 4. Law of international responsibility".

interest to investigate is the relationship between HAO:s and the peacetime regulations, i.e. State sovereignty and non-intervention, as well as what this generates in terms of breaches and violations, which triggers the State responsibility.

As has been ascertained in the above, the observation and conclusion is that international law generally applies to both of the HAO constituents (i.e. cyber attacks and information influence operations). It has also been concluded that certain forms of cyber attacks and information influence operations constitute breaches of international law, which in turn constitutes such countermeasures which aggrieved States are entitled to take, in order to respond to such a breach. While the prevalence of cyber attacks are more obvious cases of violations of sovereignty and non-intervention, information influence operations instead are more often viewed as "broader" and conducted in multiple steps. This is less surprising; the effects of information influence operations or propaganda has previously in this thesis been described as being more abstract, long-term and diffuse in nature, sometimes affecting democracy at length. Notwithstanding that it is probably hard to get around having to treat information influence operations as conducted in multiple stages to some degree, the risk is that the attritional aspect of HAO:s is lost on the international community when the effects are more diffuse in nature; at least in comparison to peacetime cyber operations, which can often be identified as a more or less distinctive act.

In sum, the final conclusion here has to be that it is possible to counter HAO:s with the peacetime regulation, at least to some extent. The available measurements can be summed up as retorsion and countermeasures in accordance with international law. The positions in literature clearly favours the inclusion of cyber attacks in the applicability in general international law, thus being able to take countermeasures against. However, the assessment made in legal doctrine is that State practice reflects that States are seemingly unwilling to categorize some influence operations as unlawful, thus eliminating the taking of valid countermeasures for the victim State. Moreover, it can be argued that the peacetime regulations are not developed to deal with operations and activities which are, and do not take hold of the attritional nature of HAO:s; this can be seen in Article 15 ARSIWA, in which preparatory actions at least *prima facie* are excluded.[247] The problem of Hostile Attritional Operations, as it has been described in the initial parts of the thesis, is just that: HAO:s are of a preparatory, attritional and malicious (hostile) character, which at least the ARSIWA seemingly have been developed to abstain from regulating.[248] Proceeding from these main

[247] Delerue, 2020, p. 243.
[248] See e.g. Article 15 of ARSIWA; Delerue, 2020, p. 243.

conclusions, the next natural step is to investigate in what way HAO:s are handled and countered according to the regulation(s) of LOAC, in order to determine if there are more suitable solutions to be adopted into a possible future modeling of *jus ante bellum*.

4 Hostile Attritional Operations in armed conflict

As has been ascertained in the above Chapter, international law can generally be argued to aim to provide prerequisites for peace, including by establishing codes of conducts between states.[249] It is, however, not considered sufficient to only focus on developing legal conditions for war prevention; war will likely always be prevalent, in one form or another, and it has therefore been necessary to develop codes of conduct for the belligerent parties of armed conflict.[250]

While having begun with outlining the handling of Hostile Attritional Operations (HAO:s) and its constituents in peacetime—as well as examining the extent to which the international community is able to deal with cyber attacks and information influence in situations occurring during peacetime—it is now time to direct the gaze towards the handling of HAO:s in armed conflict. In this Chapter, an attempt is made to examine the handling of HAO:s in LOAC in order to investigate in what way States are able to respond to cyber attacks and information influence operations once an armed conflict has erupted. The result of this examination of the handling of HAO:s within the frames of LOAC will be analyzed and discussed in Chapter 5 and 6 below be, in regards to its ability to serve as a template for the handling of HAO:s in jus ante bellum.

4.1 Introduction to the Law of Armed Conflict and Hostile Attritional Operations

4.1.1 Outlining the general application of Law of Armed Conflict

A first disclaimer needing to be presented is that, for LOAC to be actualized, it is necessary for the prerequisites of armed conflict to have been surpassed, which is when the conflict has escalated to an armed conflict by one of the parties indulging in the use of force.[251] This strict prohibition can only be set aside if the exceptions to exercise self-defense in the UN Charter's Article 51 is at hand.[252] Although jus ad bellum and pertinent question falls outside the aim and application of the thesis, it is necessary to be aware of the fact that armed conflict needs to be prevalent in order for the LOAC regulation(s) to come into action.

Once the threshold for armed conflict has been passed, the rules and principles of jus in bello and Law of Armed Conflict (LOAC) are prevailing, consisting of two complementary

[249] Thürer, 2011, p. 39.
[250] Bring et al., 2020, p. 277. See also Kolb and Hyde, 2008, p. 17.
[251] Generally, see Bring et al., 2020, pp. 275–279.
[252] This has also been dealt with in the preceding Chapter 3, section 3.4.4, together with the principles and rules of non-intervention.

branches, namely International Humanitarian Law (IHL) and International Human Rights Law (IHRL).[253] These are the main legal bodies that in this Chapter are subjected to examination in relation to their application to the respective Hostile Attritional Operations (HAO:s) constituents, namely cyber attacks and information influence operations.

4.1.2 International Humanitarian Law: rudiments and central principles

Beginning with dissecting International Humanitarian Law (IHL), an initial remark that needs to be made is that its basic principles are considered to bind all States by constituting customary law.[254] In turn, these can generally be said to consist of four main features: 1) the principle of humanity, 2) the principle of distinction, 3) the principle of proportionality and 4) the principle of military necessity.[255] The primary aim of the regulation of IHL is to protect combatants and non-combatants from unnecessary suffering, and provide a balance between military aims and minimal humanitarian impact.[256] These are also the two directorial principles of LOAC, both of which are considered to be of necessity in order for the international community to function properly.[257] LOAC and IHL are also considered to consist of another set of principles—as far as those of the treaty-based regulation goes—attributable to Geneva Law and Hague Law.[258] Geneva Law, in turn, consists of a number of conventions, four of which are considered of utmost importance when studying the field of law of armed conflict.[259] These conventions aim to protect victims of armed conflict and those vulnerable groups that are affected by armed conflict.[260] The fourth convention (IV) aims to provide protection for i.e. victims of armed conflict, and is the one which will remain in focus in this context.[261]

A central concern for IHL in general and this thesis in particular is, as mentioned above, what constitutes a state of war; what is considered *armed conflict* is also of essence when seeking to understand if a HAO can constitute an attack within the frames of IHL. Furthermore, in order to classify as an International Armed Conflict (IAC), certain criterias has to be met. This can be deciphered from the Common Article 2 of the 1949 Geneva

[253] Henriksen, 2017, pp. 284–285. See also Sivakumaran, 2010, p. 521.
[254] Henriksen, 2017, pp. 286–287.
[255] Thürer implies that there are six aspects of IHL, see Thürer, 2011, pp. 47–51.
[256] Bring et al., 2020, p. 275; Melzer, 2022, pp. 17–18.
[257] Kolb and Hyde, 2008, p. 43.
[258] Kolb and Hyde, 2008, p. 45; Henriksen, 2017, p. 285.
[259] Henriksen, 2017, p. 285.
[260] Henriksen, 2017, p. 285.
[261] Regarding the parties having ratified the AP I of the GC, see [https://ihl-databases.icrc.org/en/ihl-treaties/api-1977/state-parties?activeTab=1949GCs-APs-an d-commentaries], accessed 2024-12-13.

Conventions.[262] One such criteria is that another State must be involved, i.e. the conflict has to be *international*.[263] Another criteria is that the conflict has to be "armed".[264] In the *Tadić* case, the International Criminal Tribunal of the former Yugoslavia (ICTY) outlined a definition for what is to be considered an armed conflict; "an armed conflict exists whenever there is a resort to armed force between States or protracted armed violence between governmental authorities and organized armed groups or between such groups within a State".[265] The definition of an International Armed Conflict (IAC) can be deciphered from the Common Article 2 of the 1949 Geneva Conventions,[266] where it is stated that "the present Convention shall apply to cases of *declared war* or of any other *armed conflict* which may arise between two or more of the High Contracting Parties".[267] This is a codification of customary IHL.[268] Proceeding from this, the lingering question which will be necessary to address in the below, is if these IAC criterions are applicable to the HAO constituents of cyber attacks and information influence operations and their special kind of nature, namely being (prima facie) non-violent in nature.

4.1.3 International Human Rights: a subsidiary regulation or necessary complement?

Besides the main *jus in bello* regulation during armed conflict, i.e. the above mentioned regulation of IHL,[269] there are other regulations applicable to armed conflict, namely that of International Humanitarian Law (IHRL).[270] Regularly, when both IHL and IHRL are applicable, IHL is given primacy over IHRL due to lex specialis.[271] However, as has been ascertained in the above, IHL is not applicable to all situations—especially not in the legal area of jus ante bellum—in which case, the situation in question is instead governed by IHRL. For instance, the GC:s was not aimed at coming to terms with some sort of issue in the relationship between the State and individuals, per se.[272] Human rights regulations, instead, have from the start been differently modeled; it has stepped into the territory of concernment

[262] Tallinn Manual 2.0, Rule 82, para 1.
[263] If this criteria is not met, it is a question of a Non-International State Conflict (NIAC), which falls outside the scope of this thesis. See also Winther, 2019, p. 65.
[264] Tallinn Manual 2.0, Rules 82, para 1.
[265] *Tadic case*, ICJ, para. 70.
[266] Winther, 2019, p. 65.
[267] Emphasis added by the author.
[268] Winther, 2019, p. 65; Kolb and Hyde, 2008, p. 75.
[269] Sivakumaran, 2010, p. 521.
[270] It is nowadays "beyond question" that IHRL applies to armed conflict, see Sivakumaran, 2010, p. 530.
[271] UN Office of the High Commissioner for Human Rights (UN Human Rights), *International Legal Protection of Human Rights in Armed Conflict*, UN Doc. HR/PUB/11/01, 2011, pp. 55–58; Fidler, 2014, p. 314.
[272] Pictet (ed.), *Commentary on the Geneva Conventions of 12 August 1949*. Vol. IV, Geneva: ICRC, 1955, para 46.

in regards to the relationship between the individual and a State.[273] Moreover, in an Advisory Opinion from 2004, ICJ stated that

> "[t]he protection offered by human rights conventions does not cease in case of armed conflict, save through the effect of provisions for derogation of the kind to be found in the Article of the International Covenant on Civil and Political Rights."[274]

While the two regulations that are IHL and IHRL share some commonalities in its purpose and application, mainly in regards to "the human person",[275] the exact relationship between IHL and IHRL remains unsettled.[276] Notwithstanding this, ICJ has in the same source cited above, namely *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territories*, expressed that the relationship between the legal disciplines can be distilled into three situations: when some rights 1) are exclusively a matter of IHL, 2) are exclusively a matter of IHRL, and 3) others are matters of both IHL and IHRL.[277]

However that may be, IHL is considered to have primacy over IHRL in most situations when both regulations are applicable, due to IHL is given primacy by the lex specialis principle.[278] While IHRL applies parallel but subsidiary to IHL, the former regulation offers some advantages in regards to e.g. humane treatment.[279] For instance, it only applies in "declared war or of any other armed conflict which may arise between two or more of the High Contracting Parties" (Common Article 3, GC).[280] As has been mentioned in the introduction to this Chapter, the declaration of war is less relevant today,[281] but the GC:s are still modelled to concern certain protected people, in certain situations.[282]

---

[273] See e.g. Happold, 2013, pp. 445–446.
[274] *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory* (Advisory Opinion), ICJ Reports 136, 2004, para 106.
[275] Sivakumaran, 2010, p. 521; ICRC, Advisory Service on International Humanitarian Law, *International Humanitarian Law and International Human Rights Law: Similarities and differences*, available via [https: //www.icrc.org/sites/default/ files/document/file_list/ihl-and-ihrl.pdf], accessed 2024-11-22.
[276] See also the discussion in Bring et al., 2020, p. 281.
[277] *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, ICJ Reports 136, para 106.
[278] UN Office of the High Commissioner for Human Rights (UN Human Rights), *International Legal Protection of Human Rights in Armed Conflict*, UN Doc. HR/PUB/11/01, 2011, pp. 55–58.
[279] Sivakumaran, 2010, p. 521. Concerning, for example, disproportionately conducted warfare in regards to collateral damage, see Article 51, para 5, lit. B, AP I.
[280] See also Bring et al., 2020, p. 282, where it is emphasized that Common Article 3 of the GC:s is a "good example" on the presence of a human rights element in the IHL regulation.
[281] See Henriksen, 2017, pp. 288–289.
[282] Happold, 2013, p. 445.

Conclusively, IHRL is undoubtedly part of the armed conflict regulation and applicable to armed conflict. Of relevance to IHRL are mainly ICCPR and ICESCR,[283] with mainly the former one being of relevance in regards to cyber attacks and information influence operations, respectively. A key question generally, in regards to IHRL, is if it is applicable in the thought-of legal area of jus ante bellum, and, if so, how that application looks; this is the topic for further examination in section 4.5 and Chapter 5 below.

4.1.4 The continued disposition of the Chapter

Having hereby concluded which areas of public international law and LOAC that are of relevance when the constituents of HAO:s are executed within the frames of armed conflict, the handling of its respective constituents are being dealt with in the following sections. Notwithstanding that the main purpose of the thesis are to examine the "gray area" between peacetime and armed conflict, giving attendance to the handling of HAO:s in the regulations pertinent to armed conflict can be of use, especially when analyzing the lacks in the handling of HAO:s in jus ante bellum.

The review of two constituents of Hostile Attritional Operations are here being treated separately, beginning with the regulation (or lack thereof) of cyber attacks and information influence operations in IHL. After this, the respective constituent of HAO:s will be dealt with in regards to IHRL, before addressing the common issues of the respective HAO constituents during and some final remarks of the HAO handling in warfare.

4.2 Cyber attacks and International Humanitarian Law

As has been ascertained in the introductory parts of the thesis, cyber attacks have become an increasing headache for States and their civil societies with the entry of modern day technology.[284] Not only are cyber attacks present in the "gray area" which is presumed to take place between peacetime and warfare, they can also be used as a way of "doing warfare". Though cyber attacks, by its characteristics of "taking place in cyberspace", are *prima facie* non-violent in nature, their effects on the highly technologicalized society in which we live in today are palpable, to say the least. Using cyber attacks, hostile-intended States have the ability to take down crucial payment systems via e.g. DDos attacks, knock out power grids and disable GPS systems with imaginable detrimental consequences, inter alia. Therefore, for

[283] See e.g. the Tallinn Manual 2.0., "Part II: Specialised regimes of international law and cyberspace/6. International Human Rights Law", para 2.
[284] Schmitt, 2015, p. 1.

easily understood reasons, cyber *operations* are considered to be of significant value as a means in the toolbox of a State during armed conflict, but obviously also a threat to other States, when being a target of the cyber *attack* in question.[285]

In the following examination, questions pertinent to the issue of cyber attacks and which are aimed at being dissected further are, for example, "when are HAO:s [cyber attacks and information influence operations] prohibited and when are they permitted?", "when is a HAO considered an attack in an IHL sense?", "is use of *force* necessary for a certain conduct to be prohibited?", etcetera. This is what is attempted in the following section, with the goal at length of analysing the possibilities to use aspects of the LOAC regulations and handling of the conduct categorized as a template for a development of jus ante bellum.

4.2.1 The regulation of cyber attacks in International Humanitarian Law

Cyber attacks have, as mentioned, not received great attention in the making of treaties.[286] However, there is evidence of States having shown to consider cyber attacks as part of customary law, although cyber-specific custom is considered sparse.[287] Attempts to settle down lex lata in regards to cyber attacks have nonetheless been made in the Tallinn Manual(s) on the International Law Applicable to Cyber Operations, in regards to both peacetime, jus ad bellum and jus in bello (especially in Tallinn Manual 2.0).[288] Since it is the regulation of cyber attacks in LOAC which is the subject matter in this section, in the following, the jus in bello regulation concerning cyber attacks will be further elaborated on; this is initially done by relying on the lex lata which is outlined in the Tallinn Manual 2.0.

The Tallinn Manual 2.0 is quite clear on its position that the law of armed conflict generally is applicable to cyber attacks, when the cyber operation in question is executed "in the context of an armed conflict".[289] In the commentary of Rule 80 of the Tallinn Manual 2.0, the experts were "unanimous" in their view of cyber operations as equal to other kinds of

[285] Regarding the distinction between cyber operations and cyber attacks in LOAC, see e.g. Tallinn Manual 2.0, 2017, Rule 80 "Applicability of the law of armed conflict" and Rule 92 "Definition of cyber attack" with commentaries.
[286] "Introduction", *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, February 2017, p. 3.
[287] "Introduction", *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, February 2017, p. 3.
[288] "Introduction", *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, February 2017, p. 3. Regarding the discussion of cyber attacks in peacetime, see also above in Chapter 2. The first Tallinn Manual from 2013 was instead more focused on settling down the lex lata handling of cyber activities in armed conflict, see the foreword by Ilves in Tallinn Manual 2.0, 2017, p. xxiii.
[289] "Part IV – The law of cyber armed conflict/16. The law of armed conflict generally", in *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, February 2017, Rule 80.

operations, despite the novel nature it is characterized by.[290] According to the Manual, once there are "on-going kinetic hostilities" which in and of itself constitutes an armed conflict, all cyber operations "undertaken in relation to that conflict" will be governed by IHL.[291] Having ascertained this, it is now time to examine whether a cyber operation or attack *per se* can constitute an armed conflict.

4.2.2 Definition of cyber attack (Rule 92 Tallinn Manual)

The word "attack" carries with it connotations when operating in the regulations pertinent to armed conflict; the very concept of *attack* evokes prohibitions of conduct for the participating parties in the armed conflict, inter alia.[292] In Tallinn Manual 2.0, Rule 92–120 are supposed to reflect lex lata regarding cyber attacks as *attacks* in the IHL meaning of the word. Starting off with analysing Rule 92 of the Tallinn Manual 2.0, where it is set forth that

> "[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."

Thus, when a State participating in an armed conflict uses cyber attacks as a means of warfare, the experts define a *cyber attack* as an attack to which IHL is applicable, at least when the cyber attack in question is—as the wording goes—*reasonably expected to cause injury or death to persons or damage or destruction to objects*.[293] Consequently, the Experts of the Manual agreed that not all cyber operations qualify as cyber *attacks*; as the commentary to Rule 80 stipulates, the term "cyber operations" in the Manual include cyber attacks, but the former term is wider in its application.[294]

To elaborate on Rule 92 further, it needs to be observed that it is based on Article 49(1) of the AP I, where it is stated that "[a]ttacks means acts of violence against the adversary, whether in offence or defence". The analysis which the Experts makes in the commentary to the Manual is that Article 49(1) provides a definition where violence is what differs between attacks and other military operations.[295] However, according to the Experts, acts of violence are not considered as "limited to activities that release kinetic force".[296] The

[290] Tallinn Manual 2.0, Rule 80, para 1.
[291] See the comparison of the 2007 Estonia cyber operations versus the conflict between Russia and Georgia in 2008 in Tallinn Manual 2.0, Rule 80, para 3.
[292] Tallinn Manual 2.0, Rule 92, para 2.
[293] Tallinn Manual 2.0, Rule 92.
[294] Tallinn Manual 2.0, Rule 80.
[295] Tallinn Manual 2.0, Rule 92, para 2.
[296] Tallinn Manual 2.0, Rule 92, para 3.

Experts exemplify this position by referring to e.g. chemical or radiological attacks, which do not have a "kinetic release", while still being considered an attack in the IHL meaning of things.[297] Moreover, according to Delerue, "the prohibited force is not confined to *armed* force".[298] This is argued to be the case by leaning on the *Nuclear Weapons* Advisory Opinion, where ICJ stated that prohibition applies to any use of force, "regardless of weapons employed".[299] While Delerue emphasises that the wording of "force" does not entail "any kind [type] of force".[300] Some conduct is probably excluded from use of force, even if it instead can be considered violations of other principles.[301]

At its core, much like what the starting point is for cyber attacks in the Manual regarding peacetime, the "method and means" with which the conduct is executed has to qualify the cyber attack as an attack.[302] Means and methods, for the purposes of the Manual, are specified in Rule 103, where it is stated that means of cyber warfare are considered "cyber weapons and their associated cyber systems" (Rule 103[a]), while methods of cyber warfare are described as "cyber tactics, techniques, and procedures by which hostility are conducted" (Rule 103[b]). The terms "means" and "methods" constitute legal terms which are central to LOAC, and in the Manual, these are strictly used when referring to cyber attacks and not cyber *operations*, the latter being considered a non-legal term.[303] The follow-up question to this is when these means and methods are permissible and prohibited by IHL, and what principles and rules ultimately restrict it.

4.2.3 Cyber attacks and the principle of distinction and proportionality (Rule 93, 94 and 113 of the Tallinn Manual)

According to Rule 93 of the Tallinn Manual, "the principle of distinction applies to cyber attacks". This means that the warring parties are obligated to take precautions which honors this principle when participating in cyber attacks.[304] In regards to the general IHL prohibition of attacking civilians, the experts of the Tallinn Manual express that this is applicable to cyber attacks as well. In Rule 94 stipulates that "[t]he civilian population as such, as well as individual civilians, shall not be the object of cyber attack", while Rule 99, based on Article 52(1) of AP I, prohibits warring parties from making cyber infrastructure the object of an

[297] Tallinn Manual 2.0, Rule 92, para 3.
[298] Delerue, 2020, section 6.1.3 (emphasis added by the author).
[299] *Nuclear Weapons* (Advisory Opinion), ICJ Reports 226, 1996, p. 244, para 39.
[300] See Delerue, 2020, p. 285 f.f. (the author's remark in parentheses),
[301] Namely breaches or violations of the principles of sovereignty and non-intervention, respectively.
[302] Tallinn Manual 2.0, Rule 92, para 14.
[303] Tallinn Manual 2.0, Rule 103, para 1 and 2.
[304] Regarding the principle of distinction, generally, see Thürer, 2011, pp. 86–94.

attack it does not qualify as a military objective.[305] The prohibition of attacking civilians is further elaborated on in the commentary to Rule 93 by referring to Article 48 of the AP I, thus also being a codification of customary international law.[306] As pertains to distinction in the form of indiscriminate conduct of war, it is in both Rule 105 (indiscriminate means or methods) and Rule 111 (indiscriminate attacks) expressed that cyber attacks which are not directed at a lawful target and thus of a nature which does not, are prohibited (i.e., a prohibition from conducting indiscriminate cyber attacks).[307] The distinction between military and civilian objectives in warfare is of relevance when discussing dual-use objects, also when discussing cyber attacks and information influence which will be further elaborated in the finishing section of this Chapter.

Another principle governing IHL at large is that of proportionality, which is being dealt with in Rule 113 of the Tallinn Manual and the foundation to which can be found in Article 51(5)(b) and 57(2)(iii) of the AP I; according to the Experts, in reality, it is a question of excessiveness, rather than proportionality.[308] In Rule 113, it can be read that "[a] cyber attack that may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated is prohibited". In contrast to Rule 94 and 99, the principle of proportionality in Rule 113 instead takes aim at the situation when civilians are *incidentally* harmed.[309] According to the commentary, a cyber attack is not prohibited or unlawful automatically, due to civilians and civilian objects being harmed as a consequence of the cyber attack. Instead, the assessment of the lawfulness of the attack is dependent on a balancing act between the harm and the military advantage which the (cyber) attack is expected to generate.[310] Furthermore, according to Rule 116 (based on Article 57[2][a][ii] of AP I), the attacker should "take all feasible precautions in the choice of means or methods of warfare employed in such an attack", with regards to e.g. loss of civilian life or damage or destruction of civilian objects.[311]

---

[305] Article 52(1) of the AP I is, in turn, considered to be a codification ot the 1868 St Petersburg Declaration, see Tallinn Manual 2.0, 2017, Rule 99, para 1.
[306] See further in Tallinn Manual 2.0, 2017, Rule 93, para 2.
[307] Rule 114 is based on Article 51(1)(a)–(c) of the AP I, see Tallinn Manual 2.0, Rule 114, para 1.
[308] Tallinn Manual 2.0, Rule 113, para 1.
[309] Tallinn Manual 2.0, Rule 113, para 2. This Rule has been based on Article 51(5)(b) and 57(2)(iii) of AP I, see Tallinn Manual 2.0, Rule 113, para 1.
[310] Tallinn Manual 2.0, Rule 113, para 2.
[311] Tallinn Manual 2.0, Rule 116, para 1–3. Regarding precautions in regards to proportionality, see Rule 117. Regarding choice of targets, see Rule 118.

4.3 Information influence operations and International Humanitarian Law

4.3.1 The problem of information influence operations – a background

Moving on to information influence operations (historically, most commonly having been referred to as propaganda) which are—very much like cyber attacks with which a State or State actor, whether that be overtly or covertly, takes with the intention of it being a part of the warfare of the State in question—not only useful for States as a way of "wearing down" another State in preparations for a future armed conflict, but also as a means of warfare, once war has erupted.

Examples of States having viewed sources of information distribution as means and methods of warfare are very much prevalent in history, one of them being the NATO bombing campaign against the then Federal Republic of Yugoslavia, during which the Serbian Radio and TV Station in Belgrade was attacked on 23 of April 1999,[312] killing around a dozen civilians.[313] The purpose of the bombing—planned beforehand and intentionally executed—was according to NATO, at least in part, that the State-owned RTS was used to spread propaganda by its adversary.[314] In today's society, however, the spread of propaganda extends beyond the sender being State-owned or commercial Radio and TV Stations (RTS); with most adult individuals having access to smartphones and social media, the exposure for disinformation and misinformation is a worry to the same individuals when navigating the news cycle in cyberspace.[315] When taking place in cyberspace, the principle of distinction should apply when information infrastructures are targeted in cyberspace (see Rule 93 of the Tallinn Manual 2.0).[316] So-called Critical Information Infrastructure (CII), consisting of "computer networks and systems, the disruption or destruction of which would seriously impact health, safety, security or economic wellbeing of citizens, or the effective functioning of the government or economy"[317] have been noticed by e.g. Delerue (2020), and is also an

---

[312] Generally, see ICTY, *Final Report to the Prosecutor by the Committee Established to Review the NATO Bombing Campaign Against the Federal Republic of Yugoslavia*.
[313] ICTY, "3. Specific Incidents/iii) The Bombing of the RTS (Serbian TV and Radio Station) in Belgrade on 23/4/99", in *Final Report to the Prosecutor by the Committee Established to Review the NATO Bombing Campaign Against the Federal Republic of Yugoslavia*, para 71.
[314] ICTY, "2. Specific Incidents/iii) The Bombing of the RTS (Serbian TV and Radio Station) in Belgrade on 23/4/99", in *Final Report to the Prosecutor by the Committee Established to Review the NATO Bombing Campaign Against the Federal Republic of Yugoslavia*, para 74.
[315] World Risk Poll, "Fake News Is the Number One Worry for Internet Users Worldwide", Lloyd's Register Foundation, 2020, available via [https://wrp.lrfoundation.org.uk/explore-the-poll/fake-news-is-the-number-one-worry-for-internet-users-worldwide], accessed 2024-11-23.
[316] See also section 4.2.3 above.
[317] Delerue, 2020, p. 302; "OECD Recommendation of the Council on the Protection of Critical Infrastructure" (2008) C(2008)35.

aspect to take into account when discussing information influence operations when conducted in armed conflict.

The possible harms of disinformation to individuals have been named as mental suffering and "distortion of information vital to securing human needs", inter alia.[318] The information influence operation in armed conflict could, imaginably, concern anything from deceiving individuals that relatives have passed or been harmed, to the aggressor posing as a government official or authority and via this position instill beliefs which are harmful or dangerous to the safety and life of the individuals concerned.[319] These are also some of the thought-of concerns when discussing HAO:s in regards to IHL. In the following, the legality of information influence operations is being examined. In this context, it is perhaps most logical to begin with dissecting the Geneva Law and its Additional Protocols (AP I); most relevant perhaps being the first one from 8 of June 1977, and its article 37 that regulates the prohibition of perfidy and permissible ruses.

4.3.2 The legality of information influence operations (Article 37 of the Additional Protocol I to the Geneva Conventions)

According to the ICRC, the term "perfidy" means breaking of faith,[320] which can pose a problem within international law in both peacetime and in times of armed conflict. The concept of perfidy is quite clear: "a broken word, dishonesty, unfaithful breaking of promises, deliberate deception, covert threats", constitutes such bad faith that is intended with the use of the term in the article.[321] As can be derived from ICRC:s view of perfidy, four elements must be preexistent in order for a cyber operation to qualify as a prohibited perfidy under customary international law. The operation must 1) relate to a protection which an individual, object or activity which IHL offers protection, 2) invite confidence of the adversary which IHL prescribes it, while 3) the perpetrator has to *intentionally* betray this confidence which it has instilled in the adversary, and 4) the act has to "result in the prohibited effect of the adversary's death or injury".[322]

---

[318] Katz, "Liar's war: Protecting civilians from disinformation during armed conflict", in *International Review of the Red Cross*, 2020, p. 659.
[319] Examples of the latter can be false information of there not being water and provisions at a certain place and time, or providing wrong directions to such a place, etcetera.
[320] ICRC, *Commentary on the first additional protocol of the Geneva Conventions* (AP I), Article 37, p. 430 (General remarks).
[321] ICRC, *Commentary on the first additional protocol of the Geneva Conventions* (AP I), Article 37, p. 434, para 1497.
[322] International Cyber Law: Interactive Toolkit Contributors, "Perfidy and ruses of war" in *International cyber law: interactive toolkit*. 7 August 2021, available via [https://cyberlaw.ccdcoe.org/wiki/Perfidy_and_ruses_of_war], accessed 17 December 2024. See ICRC CIHL Study, Rule 65.

However, there is a thin line of which one situation no longer is in the scope of application of the article, at least if the conduct in question does not infringe upon international law in any clear way. In Article 37(2) of AP I, another "war strategy" than those of acts of perfidy are regulated—namely ruses—where in the Article it is stated that

> "[r]uses of war are *not* prohibited. Such ruses are acts which are intended to mislead an adversary or to induce him to act recklessly but which infringe no rule of international law applicable in armed conflict and which are not perfidious because they do not invite the confidence of an adversary with respect to protection under that law. The following are examples of such ruses: the use of camouflage, decoys, mock operations and misinformation."[323]

The use of the word "misinformation" is of interest in this context, since it suggests that it is something different from disinformation, which is often referred to when discussing information influence operations. While disinformation is a deliberate act, misinformation is considered to not carry with it the same element of intentionality in regards to the breaking of international law; to intentionally mislead an adversary (for example) in a way which does not violate international law in other aspects.[324] This raises the question of what kind of information influence operations, performed by an adversary State with hostile intent, are prohibited under AP I and its article 37(1) and 37(2), respectively. Regarding ruses, and according to ICRC:s Commentary,

> "[a] ruse of war consists either of including an adversary to make a mistake by deliberately deceiving him, or of inducing him to commit an imprudent act, though without necessarily deceiving him to this end."[325]

The wording above can be interpreted as if a State, within the framework of armed conflict and *jus in bello*, is free to distribute information and commit such information influence operations that are aimed at deliberately deceiving the adversary.[326] This interpretation is reflected in the Tallinn Manual 2.0, where certain operations directed against the civilian

[323] Emphasis added by the author.
[324] Katz, (2020) "Liar's war: Protecting civilians from disinformation during armed conflict", in *International Review of the Red Cross*, pp. 662–664.
[325] ICRC, *Commentary on the first additional protocol of the Geneva Conventions* (AP I), Article 37, p. 441 ('Second sentence — The definition of ruses of war), para 1515.
[326] Protocol Additional (I) to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts, 1125 UNTS 3, 8 June 1977 (entered into force 7 December 1978) (AP I), Art. 37(2). See also Katz, (2020) "Liar's war: Protecting civilians from disinformation during armed conflict", in *International Review of the Red Cross*, p. 664.

population are considered legal. Examples mentioned are "psychological operations such as dropping leaflets or making propaganda broadcasts", which are not prohibited, even if this conduct is directed at civilians.[327] Rule 123 of the Tallinn Manual 2.0 is based on the Article 37(2) of AP I and thus permits information influence operations conducted with cyber operations as a means.

This apparent permissibility of ruses in armed conflict are, in today's highly technologized society, questionable, considering the harms which are associated with the nature of the spreading of disinformation and misinformation.[328] For instance, Katz argues that the rules which distinguish between prohibited perfidies on the one hand and permissible ruses of war on the other hand, are not up to date with the grave ramifications of modern wartime disinformation.[329] The fact that the above mentioned wordings of the Article 37(2) defines the permissible ruse as misinformation, i.e. distinctive from the more intentional form which instead is termed "disinformation", makes the legality of the influence operations unclear, and is up for a lex ferenda discussion. However that may be, its legality at this time is exceedingly dependent on whether the information influence operation in question is to be categorized as ruse, or if it is so grave that it can be categorized as a perfidy, which usually is not the case.[330]

4.4 Cyber attacks and International Human Rights Law

4.4.1 Outlining the application: human rights in cyberspace

In previous sections, it has been concluded that States have definitely accepted or at least moved towards accepting that public international law generally is applicable to cyber attacks; International Human Rights Law (IHRL) ought to be no exception.[331] When attempting to tackle the IHRL application to the first of the two constituents of HAO, i.e. cyber attacks, in the explorative way which this thesis sets out to do, one needs to begin with imagining how cyber attacks might affect human rights. Leaning on the conclusions that have been drawn about the nature of cyber attacks in the above sections, a general starting point is that cyber attacks can pose a threat to human rights in regards to everything from the integrity of individuals, to (in the long run) the health, safety and lives of said individuals.

---

[327] Tallinn Manual 2.0, Rule 93, para 5.
[328] See e.g. Katz (2020), "Liar's war: Protecting civilians from disinformation during armed conflict", in *International Review of the Red Cross*, 2020, p. 659 f.f.
[329] Katz (2020), "Liar's war: Protecting civilians from disinformation during armed conflict", in *International Review of the Red Cross*, 2020, p. 659.
[330] ICRC CIHL Study, Rule 57.
[331] Regarding international human rights being applicable "online", see the Tallinn Manual 2.0, 2017, "Part II – Special regimes of international law and cyberspace/6. International human rights law", para 1; *The Promotion, Protection and Enjoyment of Human Rights on the Internet*, para. 1, UN Doc. A/HRC/32/L.20, 27 June 2016.

Having in section 4.1.3 outlined the bodies of law pertinent to IHRL which one needs to take into account, i.e. first and foremost International Covenant on Civil and Political Rights (ICCPR) and International Covenant on Economic, Social and Cultural Rights (ICESCR),[332] it is time to investigate in what way cyber attacks in the context pose a threat to the human rights protections of international law. In this section, the approach will be a bit different from the treatment of the subject matter in the preceding sections, mainly due to the fact that the countering of cyber attacks or (information) influence operations (or other conduct taking place in cyberspace) by States have been identified as—*in and of itself*—risking infringing upon human rights of individuals of the State in question, by e.g. restricting free speech in the name of countering influence operations.[333] However, with regards to the aim of this thesis, focus will remain on the relationship between the infringements on human rights which one State is responsible for, by targeting another State in its waging of "cyber warfare".

4.4.2 Human rights and cyber as "methods and means" of warfare

One starting point for the analysis of human rights considerations in armed conflict could be the observation that the interstate use of force per se poses a threat to human rights and its associated values.[334] Notwithstanding this being correct in and of itself, as Fidler notes, the prohibition of use of force according to Article 2(4) of the UN Charter does *not* belong to the regulation of IHRL, thus, IHL is to be categorized as something separate from human rights considerations, and the latter do not inflict on the assessment of whether a possible violation of the prohibition of use of force has taken place.[335]

Instead, human rights principles and obligations are treated and interpreted separately from IHL considerations,[336] and can to a large degree be found in ICCPR and ICESCR.[337] Just like in some cases concerning IHL, in doctrine, the application of the regulation depends on the categorization of the conduct that has occurred.[338] The 2007 cyber attacks conducted against Estonia is one example of when IHL is not applicable due to the prohibition of use of

[332] Henriksen, 2017, p. 179.
[333] See Fidler, 2014, p. 314.
[334] Fidler, 2014, p. 315.
[335] Fidler, 2014, p. 315.
[336] Fidler, 2014, p. 315.
[337] See e.g. the Tallinn Manual 2.0, "Part II: Specialised regimes of international law and cyberspace/6. International Human Rights Law", para 2.
[338] See e.g. Tallinn Manual 2.0, 2017, Rule 98 regarding terror attacks; Rule 89 regarding espionage; Rule 32 regarding peacetime cyber espionage not *per se* being unlawful.

force according to the UN Charter had not been violated; thus, IHRL ought to instead step in, in case of the presence of human rights violations.[339]

Consequently, the lingering question which follows is what *kind* of human rights violation this, in a similar situation, would constitute. In the Estonia case, the effects did not have any immediate physical consequences—harm or deaths—nor did it cause any permanent damage to civilian objects.[340] According to Fidler, such cyber attacks did not per se evoke any human rights concerns among the scholarly community; instead one could argue that cyberweapons cause less harm to human rights interests than regular weapons used in armed conflict.[341] What, if anything, would then make IHRL relevant in cyberspace? Again, one needs to return to the means and methods of the cyber attack—i.e. the cyber "weapons" used in the concrete occasion—which could be argued to infringe on human rights, depending on how they are being used. Terror attacks and espionage, for instance, would constitute such crimes and violations which cyber attacks could be used to conduct.[342] However, Fidler argues that there are few to none examples of cyber weapons being used in armed conflict in a way which invokes any serious human rights considerations, which makes *lex lata* remain unclear.[343]

Conclusively, the assessment has to lean towards cyber attacks not having any larger doctrinal implications for IHRL at this time; this, mainly because it is hard to identify specific human rights infringements due to the way cyber attacks are viewed, i.e. as at least a lesser violation of human rights than "regular" warfare. Doing so in the future would most likely encounter opposition or disinterest, based on the effects of cyber attacks in relation to human rights considerations.[344] As Fidler argues, however, if the "human rights community" were to move towards a view where, for example, internet freedom is regarded as essential to ensuring human rights, this might be a question for a *lex ferenda* discussion in the future.[345] The risk of not countering hybrid warfare can be argued to further escalating a situation, namely by normalizing activities which constitute de facto preparations for an armed conflict, which will further be elaborated on going forward.

[339] See Fidler, 2014, p. 316.
[340] Fidler, 2014, p. 316.
[341] Fidler, 2014, p. 317; 324–325; 333.
[342] See e.g. Tallinn Manual 2.0, 2017, Rule 98.
[343] Fidler, 2014, p. 299–300; 302; 310; 333.
[344] Fidler, 2014, pp. 326–327; 332–333.
[345] Fidler, 2014, p. 333.

4.5 Information influence operations and International Human Rights Law

4.5.1 Human rights and the effects of dis- and misinformation

The protection which IHRL provides to individuals also concerns information influence operations; the possible effects and consequences of information influence operations have been identified as exposure to retaliatory violence, distortion of information vital to the securing of human needs and (severe) mental suffering.[346] This has to a part been discussed in regardance to information influence operations within the framework of IHL in section 4.3; here, the particular concerns to IHRL will be addressed.

As has been ascertained in the section above, the human rights considering cyber attacks are considered sparse in its applicability. Rather, cyber attacks and weapons as a means of warfare could be argued to be *preferable* in regards to other methods and weapons, at least when they do not cause any immediate, detectable harm. But what about information influence operations; is it, perhaps, easier to recognise that information influence infringes on human rights considerations when distorted information leads to consequences in real life, and when it affects the surroundings of the individual affected (e.g. when the wrong or distorted information one individual is given has ramifications on a group of individuals, or even society)? Or is it harder, when the effects of information influence operations are more long-term and limited to diffuse and abstract concepts such as democracy, freedom of thought and speech, inter alia? It can be argued that the reality of things is that, during warfare, civilians can be exposed to disinformation and misinformation which infringes upon IHRL, which will be shown below.

4.5.2 International human rights law and the effects of disinformation and misinformation

If one were to imagine the possible dangers which disinformation and misinformation pose to human rights in armed conflict, they can range from anything from misleading information about where there are vitalities to human need—e.g. water and supplies to be gathered, or where medical care is provided—to in a more long-term and diffuse way affecting people's perception which, in turn, affects democracy and democratic societies based on disinformation and false perceptions. Influence operations, in the form of disinformation or

[346] Katz, (2020) "Liar's war: Protecting civilians from disinformation during armed conflict", in *International Review of the Red Cross*, p. 659.

misinformation, can also expose individuals to false information regarding relatives being harmed or killed, ultimately aiming to cause distress at the receiver.[347]

While IHL would be a natural place to look for these kinds of situations, it is (as mentioned) not applicable at all times, sometimes due to the fact that the threshold for armed conflict has not been reached.[348] Furthermore, according to IHL and has been shown in the above section 4.3, information influence operations are often to be categorized as a permissible ruse, and thus legal according to that branch of LOAC. However, as has been ascertained above, IHRL is supposed to be applicable in times of armed conflict, and can be looked to in cases when it can be determined that IHL does not apply. Mis- and disinformation can be argued to possibly violate human rights in certain aspects of the way it is conducted. A recent example is the way information was distorted during the Covid-19 pandemic, which ultimately infringed upon the right to life and health, if the State in which the disinformation is conducted does not take proper measurements to prevent and control the spread of diseases.[349]

Additionally, in Article 19(2) of the ICCPR, it is stated that "[e]veryone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice." According to Katz, this guarantee cannot for certain be ascribed any restraint on States from "publishing inaccurate information", etcetera.[350] However, in Article 20(1) of the ICCPR, it is likewise stated that "[a]ny propaganda for war shall be *prohibited* by law".[351] By this, the Article is—according to the Commentary on ICCPR—meant to prohibit "all forms of propaganda threatening or resulting in an act of aggression or breach of the peace contrary to the Charter of the United Nations".[352] Accordingly, States are obligated to take "legislative measurements" in order to

---

[347] Katz, (2020), "Liar's war: Protecting civilians from disinformation during armed conflict", in *International Review of the Red Cross*, 2020, pp. 679–680.
[348] See e.g. Happold, 2013, p. 445.
[349] Human Rights Committee, General Comment No. 36, "Article 6: Right to Life", UN Doc. CCPR/CGC/36, 3 September 2019, para. 26; Committee on Economic, Social and Cultural Rights (CESCR), General Comment No. 14, "The Right to the Highest Attainable Standard of Health (Art. 12)", UN Doc. E/C.12/2000/4, 11 August 2000, para. 16.
[350] Katz (2020), "Liar's war: Protecting civilians from disinformation during armed conflict", in *International Review of the Red Cross*, 2020, p. 676.
[351] Emphasis added by the author.
[352] General Comment No. 11 of the HR Committee (HRI/GEN/1/Rev.9 (Vol. I) p. 182), particularly § 2, available via [http://ccprcentre.org/ccpr-general-comments], accessed 2024-12-29; CCPR Centre, "Article 20: Prohibition of propaganda for War and Advocacy of National, Racial or Religious Hatred", in *Simple Guide on The International Covenant on Civil and Political Rights (ICCPR)*. Available via [https://ccprcentre.org/files/media/ICCPR_easy_to_read_commentary_WEB.pdf], accessed 2024-12-29.

prohibit measurements which, for example, influence the willingness of individuals to go to war if that is done by exaggerating facts.[353]

4.6 Conclusion: Hostile Attritional Operations in armed conflict

Starting off with analysing the common denominator of HAO:s, namely the fact that both cyber attacks and information influence operations are prima facie non-violent in nature, it can be concluded that the prima facie non-violent nature of the HAO constituent does *not* per se discriminate it from being part of the warfare in armed conflict. At least regarding cyber attacks, when conducted in relation to or as part of an armed conflict, IHL is applicable to the conduct taken within the frames of armed conflict.[354] Moreover, by referring to ICJ:s statements in the *Nuclear Weapons* Advisory Opinion, it can be argued that force does not necessarily demand that it would be *armed*.[355] Once the threshold for war has been surpassed, however, scholars apparently agree that IHL is applicable to HAO:s when conducted in cyberspace.[356] While the approach of the Experts of the Tallinn Manual are that cyber operations not "per se" are regulated by (general) international law (even though the method which is used to execute the cyber attack in question can *per se* be forbidden),[357] cyber attacks *are*, when they are conducted in the context of armed conflict and amounts to a cyber attack in the IHL sense.[358]

More complicated, at least *prima facie*, is the handling of information influence operations in IHL. Regularly categorized as a ruse, these kinds of operations are often permissible in accordance with 37(2) AP I. While there is probably a lot to be learned from the LOAC regulation in the modeling of HAO:s in jus ante bellum, the way in which ruses are considered in the LOAC sense of things probably needs to be reviewed, before it can serve as a model for jus ante bellum in this regard. Once revised in accordance, however, it could be an approach which would benefit the countering of information influence operations in jus ante bellum.

---

[353] CCPR Centre, "Article 20: Prohibition of propaganda for War and Advocacy of National, Racial or Religious Hatred", in *Simple Guide on The International Covenant on Civil and Political Rights (ICCPR)*. Available via [https://ccprcentre.org/files/media/ICCPR_easy_to_read_ com mentary_WEB.pdf], accessed 2024-12-29.
[354] See the Tallinn Manual 2.0, 2017, Rule 80.
[355] *Nuclear Weapons* (Advisory Opinion), ICJ Reports 226, 1996, p. 244, para 39.
[356] The Experts of the Tallinn Manual 2.0 are united in this opinion, see Tallinn Manual 2.0, 2017, Rule 80 "Applicability of the law of armed conflict", para 1, which reads that "[d]espite the novelty of cyber operations and the absence of specific rules within the law of armed conflict explicitly dealing with them, the International Group of Experts was unanimous in finding that the law of armed conflict applies to such activities during […] international […] armed conflicts […]". This can be read in contrast to the Experts approach to peacetime according to Rule 32, is that cyber operations are not "per se" regulated by (general) international law, but the method which is used to execute the cyber attack in question can *per se* be forbidden.
[357] Tallinn Manual 2.0, 2017, p. 168; Rule 32 "Peacetime cyber espionage".
[358] Tallinn Manual 2.0, 2017, Rule 80; Rule 92.

5 Jus ante bellum

Having now, at least to a certain degree, examined the regulations pertaining to Hostile Attritional Operations in peacetime and armed conflict, respectively, it is time to move on to discuss the results of this examination in the light of the suggested development of a jus ante bellum regulations and principles in international law.[359] In this thesis, the use of jus ante bellum is aimed at coming to grips with situations that—to put it simply—does not involve the prima facie use of force, takes place *before* a war has erupted, and are of attritional nature, i.e. presumed to be de facto preparations for war.

Perhaps the most obvious question that emerges, when discussing a possible change in or expansion of law, is whether there at all is a need for the suggested changes or expansion. On what grounds can one argue that a regulation of jus ante bellum is necessary? This question is the starting point for the discussion in this Chapter.

5.1 Is there a need for a jus ante bellum regulation?

In the above Chapters, the legal frameworks applicable to HAO:s in peacetime and armed conflict have been identified, outlined and examined. One question that has been aimed at being answered during this examination is how these respective legal frameworks permit the taking of countermeasures against the responsible State, and what the main challenges and uncertainties in the applicable law is in this regard. The lex lata examination of the peacetime regulations was made by leaning on the principles of sovereignty, non-intervention and State responsibility pertaining to HAO:s, with the main conclusion being that cyber attacks often warrants State responsibility, in some form or another. However, a central concern when discussing State responsibility—and information influence operations especially—is that Article 15 in ARSIWA is *not* aimed at regulating so-called "preparatory" activities,[360] which is close to what one would describe the nature of HAO:s as. Both (but mainly the former of) cyber attacks and information influence operations could be argued to classify as composite acts, at least in some cases; cyber attacks are more likely to be categorized as composite in nature, when *part* of an influence operation, in which case State responsibility is up for discussion. However, the fact that preparatory activities are excluded makes the special

[359] See e.g. Fogt (2020), "Legal Challenges or 'Gaps' by Countering Hybrid Warfare – Building Resilience in *Jus Ante Bellum*".

[360] As has been dealt with in Chapter 3, Article 15 ARSIWA prohibits "composite" acts but not when "preparatory" in nature.

treatment of "a series of actions […] defined in aggregate as wrongful […]"[361] not designed to deal with the attritional nature of HAO:s.[362]

The follow-up question is if these challenges and uncertainties warrant—or could be helped by—a conceptualization of jus ante bellum. What, then, constitutes the notion of jus ante bellum? According to Fogt, the concept of *jus ante bellum* has no firmly established meaning.[363] Purely semantic, however, its meaning is "right before war", which Fogt suggests "denotes the law applicable in peacetime or crisis prior to a possible armed conflict".[364] Other scholars have instead suggested that there are situations when the content of treaty law or other instruments can be argued to lack in regards to handling these (perceived as existing) gray areas between war and peace, in a desired way.[365] Eide et al., although almost three decades ago, has put a few areas wherein international law is lacking in regards to the question of "combating the grayzone between war and peace".[366] One case, Eide et al. argues, constitutes such a situation which falls below the threshold of applicability of international humanitarian law; another is when the concerned State is not a party of the relevant treaty (or other instrument) which contains the rules regulating the situation at hand.[367]

Another conclusion to be made of the assessment and comparison of respective regulation that has been made in the above, is that international law is either too fragmented or not adequately aligned with the particular character of HAO:s to offer anything but little helpful guidance on how the established regulations and divisions between them could be used to counter HAO:s. Thus, it could be argued, a development of jus ante bellum may bridge the gap that emerges between peacetime and warfare regulation. But how does the international community go about doing that, all while trying to deter the parties from impairing the fragile peace in an already amped up situation? This is not an easy question to have answered. As Fogt has suggested, however, to build legal resilience in a pre-war situation, it is necessary to examine the extent to which such attritional activities are already regulated in peacetime and warfare respectively, in order to assess whether there are, in fact, legal "gaps" or "gray areas" that have to be countered in the first place.[368]

---

[361] Article 15 of ARSIWA.
[362] See Crawford, 2002, p. 141.
[363] Fogt, 2020, p. 59, f.n. 79.
[364] Fogt, 2020, p. 59.
[365] See e.g. Happold, 2013, p. 444.
[366] Eide et al., 1995, p. 217.
[367] Eide et al., 1995, p. 217. Regarding this issue as it pertains to treaties in the area of IHRL, see the Tallinn Manual 2.0, "Part II Specialised regimes of international law and cyberspace/6. International human rights law", para 2.
[368] Fogt, 2020, p. 99.

Lastly, in regard to the question of a presumed need for a legal area called jus ante bellum, its relation to jus contra bellum (the law against war) needs to be addressed. In this thesis, it is recognised that the description of jus ante bellum here shares some similarities with the aim of jus contra bellum; it needs to be aimed towards curb international use of force and protect global peace. However, by using jus ante bellum to highlight the issues which take place in the space between war and peace, it is easier to model the solutions to work towards the goal of protecting international stability, security and human rights. Jus contra bellum is not rejected, in fact, here, it is very much regarded as useful; jus ante bellum can perhaps be described or suggested to constitute a subcategory to jus contra bellum, especially aimed at dealing with war preparatory activities which poses dangers to the *erga omnes* obligation of aiming at protecting international peace.

5.2 Jus ante bellum and the fragmentation of international law

As has been previously discussed, the current issue of fragmentation of international law has—inter alia—the effects of making international law as a whole more patchy and contradictory, and thereby making it harder to overview, navigate and, long-term, apply.[369] When the fragmentation instead causes an over-regulation of international law, it carries with it consequences of conflicting and incompatible rules and principles.[370] While the fragmentation problem in international law has been offered solutions by the ILC, in the form of principles of interpretation, inter alia, it deserves some elaboration in regards to jus ante bellum in this context.[371]

One goal of regulating jus ante bellum must therefore be to not aggravate the problem of fragmentation in international law further; preferably, a jus ante bellum can contribute to the opposite, namely to serve as a bridge between peacetime and armed conflict in order to eliminate uncertainties and unwanted “gaps” or “gray areas", which States with malicious or hostile intent seeks to take advantage of. This notwithstanding, it is a complicated task to aim to be completely sure that a sketch of jus ante bellum starts where the peacetime regulations ends and stops where jus ad bellum and subsequently armed conflict begins; this does not mean that a legal area of jus ante bellum per se is unnecessary or redundant, just that it is probably not achievable to strive to establish a legal framework where there is a definite “end

[369] See, generally, “Fragmentation of international law: Difficulties arising from the diversification and expansion of international law” (ILC, A/CN.4/L.702, 2006).
[370] ILC, A/CN.4/L.702, 2006, p. 5.
[371] ILC, A/CN.4/L.702, 2006, p. 5.

and beginning". For example, it would not be "in vain" to argue that the use of jus ante bellum is necessary in order to highlight issues with the respective framework of peacetime and armed conflict and their inherent challenges when it comes to countering HAO:s, or that the result necessarily has to result in excessive regulation. Some overlapping does not pose a problem to the degree that it would be an issue in the application; also, there are interpretative methods in place to help determine when the respective regulation should be given primacy, which the author of this thesis see no obstacle in applying to jus ante bellum and its adjacent legal areas.[372]

5.3 Special legal challenges of jus ante bellum

Some special legal challenges in just ante bellum noteworthy deserves to be further elaborated on. Information influence operations, sometimes called "informational campaigns" or "psychological operations",[373] can sometimes be conducted by information campaigns consisting of fake news aimed at influencing the citizenry in the victim State, i.e. *disinformation*. According to Fogt, these types of campaigns do not amount to an attack in the LOAC sense of things, however, they can constitute an unlawful "threat of attack or other unlawful acts under international law";[374] this, if the hybrid information influence operation encourages "the commission of acts contrary to general principles of humanitarian law".[375] One conclusion Fogt makes is that the most effective measures against such hybrid information influence operations and "propaganda 'lawfare'" is to hold on to the rule of law and educate the citizenry about the hybrid warfare and its inherent threats, in order to build "civilian, political and legal resilience".[376] However, to achieve this, it probably needs to be accompanied by State practice which reflects the seriousness of attritional, preparatory activities in jus ante bellum, maybe by leaning on the LOAC regulation in some aspects.[377]

Moreover, there are some lingering concerns regarding International Human Rights Law (IHRL), which in this thesis has been treated in connection to armed conflict, and as part of the LOAC regulation. Noteworthy is that IHRL has a wider application than being strictly limited to LOAC—in fact, it is considered to be applicable at—which technically would make

[372] Lex specialis and Article 31(3)(c) (regarding systemic integration) of the VCLT are examples of solutions for future conflicts of applicability; regarding the latter, generally, see Merkouris, *Article 31(3)(c) VCLT and the Principle of Systemic Integration*, 2015.
[373] See Fogt, 2020, p. 97.
[374] Fogt, 2020, p. 97.
[375] Fogt, 2020, p. 97.
[376] Fogt, 2020, p. 97.
[377] See further in section 5.5 below.

IHRL applicable in the legal area of jus ante bellum as well. It is clear that both cyber attacks and information influence operations affect human rights, the latter being affected by Article 20(1) of the ICCPR, i.e. the prohibition of war propaganda.

As has been mentioned, however, according to Fidler, the human rights community has tended to put less emphasis on hybrid warfare in the shape of cyber attacks or information influence operations, as the consequences in contrast to "regular" warfare have been less obviously dire.[378] It is in its place here to reiterate that if the dangers of HAO:s in jus ante bellum which has been worded in this thesis were to be realized, human rights would indeed also be threatened in the long run. This demands of the scholars to not only recognize that hybrid warfare in the shape of HAO:s can pose a threat to human rights in jus ante bellum, but probably also that cyber attacks and information influence operations is just a tool in a hostile-intended State's toolbox, and sometimes constitutes de facto preparations for a potential armed conflict.

5.5 Lended principles and handlings for jus ante bellum

The question, which has previously been posed, is whether the armed conflict handling of HAO:s could be a good fit for the modelling of the ditto in jus ante bellum, in one or more aspects. One concern is that a regulation of HAO:s in jus ante bellum would counteract one of the aims of both public international law generally and the proposed purpose of jus ante bellum specifically, namely global peace, stability and security. By suggesting an expansion of the scope international law, there are imaginable risks to international peace, especially if the expansion contains suggestions on further countermeasures, which the aggressor interprets (or chooses to interpret) as an escalation, and refers to when attempting to justify harsher methods in its waging of hybrid warfare—or even uses as an excuse to exercise its right to self-defense in accordance with Article 51 of the UN Charter. This is a practical problem when navigating regulations adjacent to war-like states or situations, and this probably needs to be considered in relation to the fact that experiences from history have shown that tangibility in regards to States with malicious intent in fact can escalate tensions and the resorting to violence, as a means to "still the hunger" for changing borders by force.

While principles of e.g. non-intervention and sovereignty prevails in the peacetime regulation, the principles of distinction, proportionality and necessity also apply to the taking

[378] Fidler, 2014, pp. 326–327; 332–333.

of countermeasures by an aggrieved State.[379] However, when States with hostile intent operates in peacetime and finds "gray areas" to act in accordance with the Lotus dictum—meaning that "what is not prohibited is permitted"—a lot of unwanted (although permissible) State conduct or "hybrid warfare" is disconnected from principles which could limit the injury or harm done, at least in theory. It bears repeating that unfriendly State conduct not *per se* is prohibited;[380] and if hybrid warfare is not prohibited or unlawful, it is not restrained by principles aiming to lessen its consequences. Moreover, the sketching of jus ante bellum could benefit from—for instance—adopting the principles of proportionality and necessity from both the handling of HAO:s in peacetime and armed conflict, in order to achieve the presumed goal of not wanting to escalate tensions in international relations further.

5.6 Conclusions: Hostile Attritional Operations and jus ante bellum

Before continuing on to the final analysis of the thesis, it is now in place to return to the question constituting the starting point for this Chapter, mainly whether it is pursuable to establish the thought-of concept of HAO in jus ante bellum. First, is the concept of Hostile Attritional Operations at all needed? There are already several concepts occurring in international law which are addressing the problems of hybrid warfare; some of which have been discussed in the preceding Chapters. Notwithstanding that such concepts deals with, the specific concept of HAO:s is aimed at dealing with a certain *form* or *type* of hybrid warfare, namely the issues that prima facie falls below the threshold for armed conflict and are of attritional nature, thus often being "left hanging" with the legal framework of peacetime. This is something which can be argued to be deficient for the task of countering HAO:s in the area of jus ante bellum, at least if one decides to put emphasis on the fact that the attritional "preparatory" activities which HAO:s are thought to consist of, and are going on in the gray area between war and peace, are lost on the international community and regulations.

A final conclusion in regards to the necessity of a jus ante bellum is that it probably can end up overlapping adjacent legal areas, however, this is probably a less extensive problem, as there are methods of e.g. interpretation in international law, which could help curb such issues. Lastly, a modeling of jus ante bellum needs to include jus contra bellum aspects, i.e. its aim should exceedingly be to prevent the outbreak of armed conflict, which

[379] See e.g. Delerue, 2020, especially subsections 10.2.3.1 "Necessity"; 10.2.3.2 "Proportionality".
[380] Tallinn Manual 2.0, 2017, Part Chapter 5, "Cyber operations not *per se* regulated by international law", p. 168.

needs to be modelled with the risk of escalation in mind. The acknowledgment of this aim benefitting from clear and firm State practice and doctrine on how to relate to and counter hybrid warfare, nonetheless, is also central to the shaping of the legal area of jus ante bellum.

6 Analysis

Above, the handling of HAO:s according to respective frameworks of peacetime and armed conflict have been examined and described; in part to map out an assumed "gap" or "gray area" existing between the two regulations, in part to look at how aspects of the armed conflict can be drawn from and "lended" to a proposed jus ante bellum regulation. Following this, the mapping of jus ante bellum (and HAO:s in jus ante bellum more specifically), has first off been replenished by doing a lex lata investigation of the extent to which the peacetime regulations are able to come to terms with the hybrid problem which is presumed to exist between "war and peace". Second, the settling down of the handling of HAO:s in armed conflict have been examined in order to determine whether it could be a good fit for modelling the jus ante bellum regulation, at least in some regards.

6.1 The handling of Hostile Attritional Operations in peacetime

Peacetime regulations pertinent to HAO:s involves the question of attribution, (violations of) State sovereignty and non-intervention, inter alia, and has to be read in the light of tenets such as bona fide (good will, here in international relations) and pacta sunt servanda ("agreements shall be kept").[381] It is, however, not possible to answer how HAO:s are handled in the peacetime regulations of international law, without regarding some of the particular characteristics and regulations that only apply to cyber attacks and information influence operations, respectively, and making assessments accordingly. In the following sections, a final analysis of the handling of cyber attacks and information influence operations in peacetime is being made, as well as the handling of the same HAO constituents during warfare.

Beginning with cyber attacks, which according to Delerue and the Tallinn Manual are—although not being regulated as well in treaties, or even as evident from opinio juris and State practice as one searching for answers in this legal area would like—not an enigma in international law, and most authoritative authors in on the fact that international law applies to cyber-specific questions.[382] Notwithstanding the main problem of cyber attacks in peacetime (or in armed conflict, for that matter) being attribution, there is firm guidance on how to handle cyber attacks that are "provable", mainly by looking at the handling of attribution in

[381] Regarding the principle of pacta sunt servanda in international law, see e.g. Crawford, 2019, p. 434.
[382] "Introduction", in *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge: Cambridge University Press, February 2017, p. 4.

accordance with ARSIWA. There is also the Tallinn Manual[383] to look to for guidance on how to handle specific issues arising from cyber attacks; even though it does not have the authority as the ARSIWA has been recognised as having, it has as its stated purpose to determine lex lata on the subject matter (and to avoid reflecting lex ferenda).[384] As has been concluded in Chapter 3, there are also countermeasures available for an aggrieved victim State to take when exposed to HAO:s in peacetime, even if some of it would constitute retorsion, which does not constitute a breach of international law and thus, not warranting any *valid* countermeasures.

As per above conclusions, information influence operations are of a slightly different nature than that of cyber attacks. What makes the different conducts relevant to lump together can be argued to be the fact that they are a) conducted in "cyberspace", b) *prima facie* non-violent (they does not cause any immediate harm), and c) attritional, in the way that they are aimed at wearing down the resilience of a State as preparations for an upcoming war, that the hostile-intended State has in mind. Information influence operations are characterized by the fact that their effects are more long-term, but still affects the sovereignty of a State as well as possibly constituting a breach of non-intervention, mainly by intervening in other States internal affairs.

6.2 The handling of Hostile Attritional Operations in Law of Armed Conflict

A reality that has to be emphasized and yet again repeated, is that it is—due to the nature of HAO:s—hard to definitely prove whether a conduct can be attributed to the State, which has already been discussed in the previous chapters. Here, the author is proceeding with the assumption of the attribution question already being solved, i.e. that it is possible to respond to the HAO in question as if the conduct in question can be (and have been) attributed and proved to have been conducted by a certain State.

As has been discussed and finally ascertained in the Chapters above, cyber attacks are *not* exceptions from which international law would not be applicable; international law is generally applicable to cyber attacks, both in the jus ad bellum and jus in bello sense.[385] Information influence operations, also known by its more generic name of "propaganda", are

[383] Here, the Tallinn Manual 2.0 is the intended reference.
[384] "Introduction" in *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, February 2017, p. 2–3.
[385] "Introduction", in *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, February 2017, p. 5.

in the global world scene of today usually conducted on the internet (or "cyberspace", as it has been called throughout the thesis). Information influence operations that take place within an armed conflict, sometimes as a part of the warfare conduct, are governed by IHL. The crux is that information influence operations often, as part of IHL, are viewed as a permissible ruse, even though it is directed towards the civilian population.

IHRL, being a body of law which to a large part applies in parallel to IHL, does not require that an armed conflict is present to be applicable. Thus, IHRL should apply in the presumed legal area of jus ante bellum as well, when the conduct is of "hybrid" nature, i.e. non-violent and below the threshold for armed conflict. The criticism here is in some regards directed towards the human rights community and scholars, which could engage more in the threats and dangers to human rights which hybrid warfare, cyber attacks and information influence operations poses. Here, it is necessary to reiterate the importance of recognising the attritional and preparatory nature as threats to human rights. Arguably, one starting point in this context could be to pinpoint the various challenges and difficulties with IHL, where IHRL instead could develop to meet or heal these lacks in the IHL framework.

6.3 Bridging the gap: can a development of jus ante bellum help counter Hostile Attritional Operations?

As has been accentuated above, the question of whether jus ante bellum principles can help counter HAO:s demands that one is willing and able to take on the viewpoint of the attribution question being out of the way, even though it is a highly relevant concern for the practical countering of hybrid warfare that consist of cyber attacks and information influence operations. Jus ante bellum, at least according to the author of this thesis, must be built on the premise that global peace is worth preserving, and the rules and regulations therewithin should be aimed at not escalating a not yet erupted "total" war. It has earlier been suggested, the handling of HAO:s could benefit from doctrinally, i.e. within documents of NATO member States, and thus contributing to creating and developing State practice, which the international community as a whole would benefit from in regards to its effects on international peace, stability, security and respect for human rights.[386]

[386] Generally, especially regarding cyber attacks, see the conclusions made by Fogt (2020), "Legal Challenges or 'Gaps' by Countering Hybrid Warfare – Building Resilience in *Jus Ante Bellum*".

6.4 Review of the research questions

This thesis has, primarily, been aimed at conceptualizing Hostile Attritional Operations (HAO:s), in the light of developing jus ante bellum principles. This has been done by describing, comparing and analyzing how the legal frameworks of public international law in regards to peacetime as well of that of warfare, regulates HAO:s—consisting of cyber attacks and information influence operations, which are aimed at the attrition of the national defense of the State—in order to determine if these kind of attrition acts stemming from hostile foreign States offers an adequate protection for the subject State and its civilians, or if there is a "gap" or "gray area" that needs to be countered. The following research questions have been aimed at being answered:

1. What are the legal frameworks applicable to HAO:s in peacetime and in armed conflict, respectively?
2. How do these legal frameworks permit the taking of countermeasures against a State responsible for a HAO in the respective frameworks of peacetime and armed conflict? What are the main challenges and uncertainties in applicable law in this regard?
3. Could a conceptualization of HAO:s in a developing legal framework *jus ante bellum* contribute to the overcoming of challenges and uncertainties in the legal framework applicable to countermeasures?

Considering that there are several relevant questions pertinent to the peacetime state of things, it has been necessary to do an inventory of the peacetime regulations. First, the legal framework of peacetime can be ascertained to consist of a varying amount of regulations; it is those pertinent to the concepts of, for instance, State responsibility, State sovereignty and non-intervention, which also are the ones identified as relevant for the peacetime regulation pertaining to HAO:s. Moreover, while the problem of attribution cannot be overlooked, to form a perception of how the legal framework "should" be modeled with regards to an analysis that has been been performed from a lex ferenda point of view, it is also necessary to take on the viewpoint and assumption of the attribution question already being out of the way (i.e. solved). When it is possible to prove that a State has been responsible for executing a

HAO and thus being able to attribute[387] a certain hostile conduct to the responsible State in question, whether that be in peacetime or within its conducting of warfare, it is also possible to hold the State in question accountable for violating an obligation, when constituting an internationally wrongful act or a violation of LOAC. Usually, when the conduct is executed within warfare that is governed by LOAC (i.e., IHL and IHRL), there is for the most part a solid legal framework that can be used to counter attritional operations and activities. Still, this is of little use when the situation involves pre-war conduct which does not amount to an aggression or attack, and which in turn evokes the *jus in bello* regulations. As has been concluded, there are several countermeasures (including retorsion) which are available for HAO:s conducted in peacetime. However, there are some concerns in regards to the preparatory and attritional nature of cyber attacks and information influence operations, with mainly the latter one at risk of being categorized as either a permissible preparatory act (in peacetime, according to Article 15 of the ARSIWA) or as a permissible ruse in armed conflict. The suggestion here could be, for example, to review the permissibility of ruses in armed conflict, before letting it serve as a template for the handling of HAO:s in jus ante bellum.

Second, as regards to the question of the importance of establishing a concept called Hostile Attritional Operations to highlight the issues of State conduct which is may overlooked in the the regulations, it is possible that this can be accomplished by developing jus ante bellum principles further than that which is the state of things today. There are, however, several arising problems that come with an expansion of international law, which has been mentioned in the preceding Chapters. One issue at hand is the fragmentation of law, which not only makes it harder to overlook and navigate international law, but it has the long-term consequence of it being harder to study, integrate and, therefore, also apply.[388] This, however, probably constitutes a concern of lesser extent in regards to the establishment of jus ante bellum.

Third, in parallel with the issues pertinent to the fragmentation of international law, it is important to keep in mind the importance of building legal resilience jus ante bellum in a way that does not endanger international peace, security and stability, when working with developing the legal area which takes place in a pre-war situation. The main issue at hand being the escalation risk, which consist of the aspiration of avoiding both an arms race and the

[387] It is in its place to yet again remind the reader that *attribution*, first and foremost, is a legal concept of public international law pertaining to the peacetime regulation and State responsibility, thus used in regards to determining responsibility for internationally wrongful acts (the Chapter 3 above). Still, attribution has also semantic ties to questions pertinent to questions of evidence and what is able to "prove".

[388] See, generally, International Law Commission, "Fragmentation of international law: Difficulties arising from the diversification and expansion of international law" (ILC, A/CN.4/L.702, 2006); Shaw, 2021, pp. 58–59.

dangers of misperceiving other States' intentions with its countering measures. However, it is also of major importance to be aware of the fact that there are risks with *not* countering e.g. violations of State sovereignty, non-justifiable interventions and harms that are to democracy, even if this is accomplished by prima facie non-violent means that does not amount to aggressions and thus are limited to attempting to demand liability for hostile attritional activities or "behavior".[389] As has been alluded to in the Chapters above, one does not at all have to go so far as to suggest that a conduct on a par with the NATO handling of the crisis on Balkan—i.e. the bombing of the Radio Television of Serbia in April of 1999, inter alia—should be a desirable countering of HAO:s, in order to move towards a development which addresses the issues which an aggrieved State face as a consequence of de facto hostilities conducted by an adversary State. What should be an adequate response to a HAO according to the international community needs to start with States willing to develop State practice. This can be done by expressing positions, e.g. through doctrinal documents and other international or inter-State agreements; as is clear from the reality of international relations, doctrine has a de facto effect on State "behavior" and, in turn, how other States have decided to shape their own doctrine.[390]

[389] This is what many military experts view not only the Russian aggression in Georgia and Ukraine to be a result of, but also the conduct of certain actors in the Second World War; as is widely known, this was one of the more or less overtly expressed goals of Hitler and his brutal aggressions, genocide and advances throughout Europe, i.e. to make "Lebensraum" for Nazi-Germany, which was not countered as early or as firmly as it should have been, see regarding the "Final Solution" and the Molotov–Ribbentrop pact in e.g. Snyder, 2010, Chapter 4 and 6.
[390] One recent example of this is the regard of which the international community pays to States armed with nuclear weapons, and their doctrine on the use of these kinds of weapons; perhaps most talked about in recent days is Russia's "red line" for the use of nuclear weapons, which the Kremlin uses to deter Ukraine-allied States from contributing with military resources, see e.g. "NATO's nuclear deterrence policy and forces" (last updated: 30 Nov. 2023), available via [https://www.nato.int/cps/cs/natohq/topics_50068.htm], accessed 2025-01-03; Reuters, "Putin draws a nuclear red line for the West", 2024-09-27, available via [https://www.reuters.com/world/europe/putin-draws-nuclear-red-line-west-2024-09- 27/], accessed 2025-01-03. See also Hollis, 2007, pp. 1060–1061.

7 Finishing remarks and suggestions on further research

"An ounce of prevention is worth a pound of cure." — Benjamin Franklin[391]

The question of whether Hostile Attritional Operations should be a pursuable concept for the developing of jus ante bellum principles within international law, needs to be answered after a careful consideration of attribution aspects, the protection of global peace and the risks and complications of fragmentation of public international law, inter alia. The legal resilience towards pre-war conduct consisting of HAO:s seems to demand that something has to be done to counter the challenges of ill-willed States, which slowly but surely are wearing down a variety of systems that are important to society and, exceedingly, democracy itself, which is what is concerning security and military experts with e.g. Russia's increasingly aggressive behavior towards EU and NATO member States.

One conclusion to be made here is that there is still what is here called a "gap" or "gray area" which, not surprisingly, to some extent is caused by HAO:s not constituting a violent enough measure (prima facie) that warrants the right to respond with violence or military means. However, the main pursuit of a jus ante bellum is not, for that matter, necessarily to justify violence but rather to avoid it, and to build legal resilience in jus ante bellum and respond with means *adequate* for the task on hand, which in turn (exceedingly) takes aim at promoting global peace.[392] As history has shown—while one of course has to be wary of the risk of a conflict escalating into becoming a cycle of violence which everyone wants to avoid—to not deter advances (however non-violent in nature) before the hostile intended regime of a country decides to take ambiguous response to its "approaches" as an invitation to make further advances,[393] also entails risks of escalating the situation at hand. The Commission of ICISS did, already in 2001, identify the issues of not preventing a potentially deadly conflict by "quelling it in its bud".[394] The risks accompanied with leaving the area of jus ante bellum unregulated is, furthermore—in parallel to the human rights regulations and international law as a whole risk being eroded—that hybrid warfare is

[391] Cited in South Southwest PTTC, "Measuring an Ounce of Prevention and a Pound of Cure", available via [https://pttcnetwork.org/measuring-an-ounce-of-prevention-and-a-pound-of-cure/#:~:text=%E2%80%9CAn%20ounce%20of%20prevention%20is,%E2%80%9D%20and%20the%20%E2%80%9Cpound.%E2%80%9D], accessed 2024-12-29.

[392] See the definition of jus ante bellum in section 2.2; Chapter 5.

[393] Russia's illegal annexation of Crimea in 2014—and later the full scale invasion of Ukraine in February 2022—is maybe the "prime" example of such gradual, hostile-intended State conduct, that does not start with exercising violence, and to which the meek response from the world community does not deter the hostile-intended State in question from further escalation, with more dire consequences.

[394] ICISS, *The Responsibility to Protect: Report of the International Commission on Intervention and State Sovereignty*, December 2001, p. 20 f.f.

escalated from non-violent, or non-deadly, conflict to a situation where the effects of the warfare turns out to be, in fact, deadly and violent, even if prima facie non-violent.[395] Here, the human rights community could contribute to the paying of attention to the dangers which e.g. cyber attacks and information influence poses in the to human rights in jus ante bellum.

Lastly, some suggestions on further research pertinent to the subject matter of this thesis are in place. The thesis has primarily been aimed at establishing Hostile Attritional Operations as a jus ante bellum concept, but does not leave the reader with concrete suggestions on *how* jus ante bellum de facto should be developing—or how to implement Hostile Attritional Operations as a concept within public international law (other than that it highlights the fact that Hostile Attritional Operations pose a very real problem, and that the phenomenon of hostile attrition in jus ante bellum is of relevance for international law in building resilience in the "gray area" between peacetime and warfare). More concrete suggestions on how to counter HAO:s could be of use, e.g. to determine if there are aspects of the cyber defense of NATO countries that warrants more steadfast guidance on how to operate in jus ante bellum. Also, it would be of interest to further examine and delve deeper into the specific dangers which artificial intelligence (AI) could pose as a pre-war conduct (i.e., in jus ante bellum), and therefore constituting a form of HAO:s. Here, there is plenty of room for modifying the concept of HAO:s to include other attritional activities as one sees fit, in order to accomplish the task of treating e.g. AI as a HAO and perhaps even leaving concrete suggestions on how to counter such hostile attrition that is conducted States with hostile (or "malign") intent against aggrieved, or perceived adversary, States.[396] The expansion of NATO and the growing problems of attritional non-violent conduct of a State, aimed at wearing down the defense of another which de facto constitutes preparations for an upcoming war in the mind of the aggressor, surely demands a bridging of the gap which is the—for the most part—currently unregulated area of jus ante bellum.

---

[395] Aftonbladet, "Natotoppens oro: Varnar för rysk hybridattack med många döda", 2024-12-29, available via [https://www.aftonbladet.se/nyheter/a/zAQdLb/natotoppens-oro-varnar-for-rysk-hybridattack-med-manga-doda], accessed 2024-12-29.

[396] See, for example, how the Donald Trump presidential campaign of the U.S. 2024 election is toeing the line (if not fully passing it) to disinformation by using AI to seem as if celebrities are endorsing him as their candidate, in The Guardian, "How did Donald Trump end up posting Taylor Swift? AI images posted to Truth Social bore the watermark of a tiny Texas non-profit looking to bankroll X users", 2024-08-26, available via [https://www.theguardian.com/technology/article/2024/aug/24/trump-taylor-swift-deepfakes-ai], accessed 2024-10-07; Wired, "Russian Propaganda Unit appears to Be Behind Spread of False Tim Walz Sexual Abuse Claims. The Russian-aligned network Storm-1516 has a long history of posting fake whistleblower videos—including deepfakes—to push Kremlin talking points", 2024-10-21, available via [https://www.wired.com/story/russian-propaganda-unit-storm-1516-false-tim-walz-sexual-abuse-claims/], accessed 2024-10-22. See also Cristiano et al., *Artificial Intelligence and International Conflict in Cyberspace*, 2023.

Bibliography

International documents

Treaties[397]

UN General Assembly, *International Covenant on Economic, Social and Cultural Rights*, United Nations, Treaty Series, vol. 993, p. 3, 16 December 1966 [cit. "ICESCR"].

UN General Assembly, *International Covenant on Civil and Political Rights*, United Nations, Treaty Series, vol. 999, p. 171, 16 December 1966, International Covenant on Civil and Political Rights [cit. "ICCPR"].

United Nations, *Statute of the International Court of Justice*, 18 April 1946 [cit. "ICJ Statute, 1946"].

United Nations (UN), *Charter of the United Nations*, 24 October 1954, 1 United Nations, Treaty Series XVI [cit. "UN Charter, 1 UNTS XVI, 1954"].

United Nations (UN), Vienna Convention on the Law of Treaties, 23 May 1969, Treaty Series, vol. 1155, p. 331 [cit. "(the) Vienna Convention, 1969"].

European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, 4 November 1950, European Treaty Series 5 [cit. "ECHR"].

Rome Statute of the International Criminal Court (last amended 2010), 17 July 1998 [cit. "ICC Statute, 1998/2010"].

Resolutions

General Assembly Resolution 217 A (III), Official Records of the third session of the General Assembly, Part I, 21 September – 12 December 1948, Resolutions (UN doc. A/810), pp. 71–77 [cit. "UNGA Resolution 217 A (III)"].

General Assembly Resolution 1514 of 1960, *Declaration on the Granting of Independence to Colonial Countries and Peoples*. A/RES/1514(XV), 14 December 1960 [cit. "UNGA Resolution 1514 (XV)"].

General Assembly's Resolution 2131 (XX), *Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of Their Independence and Sovereignty*, 21 December 1965 [cit. "UNGA Resolution 2131 (XX)"].

General Assembly Resolution 2625 of 1970, *Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations*. A/RES/2625(XXV) (25th session: 1970), 1971 [cit. "Friendly Relations Declaration"].

General Assembly's Resolution 3314 (XXIX), *Definition of Aggression*. A/RES/3314(XXIX), 14 December 1974 [cit. "UNGA resolution 3314 (XXIX)"].

[397] Includes conventions, statutes, protocols, etc.

Other (UN) documents

OECD, "Recommendation of the Council on the Protection of Critical Infrastructure", 2008, C(2008)35.

UN Doc. HR/PUB/11/01, UN Office of the High Commissioner for Human Rights (UN Human Rights), *International Legal Protection of Human Rights in Armed Conflict*, 2011, pp. 55–58.

UN Doc. S/2022/1544 *Letter dated 24 February 2022 from the Permanent Representative of the Russian Federation to the United Nations addressed to the Secretary-General*. Annex to the letter dated 24 February 2022 from the Permanent Representative of the Russian Federation to the United Nations addressed to the Secretary-General. Address by the President of the Russian Federation.

UN Doc. E/C.12/2000/4, Committee on Economic, Social and Cultural Rights (CESCR), General Comment No. 14, *The Right to the Highest Attainable Standard of Health* (Art. 12), 11 August 2000.

UN Doc. A/HRC/32/L.20, *The Promotion, Protection and Enjoyment of Human Rights on the Internet*, para. 1, 27 June 2016.

Human Rights Committee, General Comment No. 36, "Article 6: Right to Life", UN Doc. CCPR/CGC/36, 3 September 2019, para. 26

Commission reports[398]

International Commission on Intervention and State Sovereignty (ICISS), *The Responsibility to Protect: Report of the International Commission on Intervention and State Sovereignty,* December 2001.

International Law Commission, *Report of the International Law Commission*. Fifty-fourth season, supplement no. 10 (A57/10) Geneva: 29 April–7 June and 22 July–16 August 2002 [cit. "ILC, General Assembly, A/57/10 suppl. 10, 2002"].

International Law Commission, *Fragmentation of International Law: Difficulties Arising from the Diversification and Expansion of International Law. Report of the Study Group of the International Law Commission, Finalized by Martti Koskenniemi*. Fifty-eighth session, Geneva: 1 May; 9 June 9; 11 August 2006 [cit. "ILC, A/CN.4/L.682"].

Court cases

International Court of Justice (ICJ) cases[399]

Corfu Channel Case (UK v. Albania) (Merits) ICJ Reports 4, 1949.

Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), ICJ Reports, 1986.

Legality of the Threat or Use of Nuclear Weapons (Advisory Opinion) ICJ GL No 95 [1996], ICJ Reports 226, ICGJ 205 (ICJ 1996), 8th July 1996.

[398] Includes documents from the International Law Association, International Law Commission (ILC) and International Commission on Intervention and State Sovereignty (ICISS).
[399] This section also includes ICJ:s Advisory Opinions.

Gabčíkovo-Nagymaros Project (Hungary v. Slovakia) (Judgement), 1997, ICJ Reports 88.

LaGrand case (Germany v. United States) (Judgement) ICJ Reports 466, 27 June 2001.

Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory (Advisory Opinion), International Court of Justice [ICJ], 2004.

Accordance with international law of the unilateral declaration of independence in respect of Kosovo, Advisory opinion, ICGJ 423 (ICJ 2010), 22nd July 2010, International Court of Justice [ICJ] [cit. "ICJ, Advisory opinion on the declaration , 2010"].

Application of the Genocide Convention (Croatia v. Serbia), ICJ Reports 2008, General List No. 118, 18 November 2008.

Permanent Court of International Justice (PCIJ)[400]

Lotus Case (France v. Turkey), (Judgement), Judgment No 9, PCIJ Series A No 10, ICGJ 248 (PCIJ 1927), (1935) 2 Hudson, World Ct Rep 20, 7th September 1927, League of Nations (historical) [LoN]; Permanent Court of International Justice [PCIJ].

Factory at Chorzów (Merits) (Judgement), PCIJ Series A No 17, 8 February 1927/13 September 19, Permanent Court of International Justice [PCIJ].

International Criminal Tribunal for the former Yugoslavia (ICTY) cases and reports

ICTY, *Prosecutor v. Duško Tadić* (Judgement). Case No. IT-94-1-Tbis-R1117, 11 November 1999.

ICTY, *Prosecutor v. Naletilić and Martinović* (Judgement). Case No. IT-98-34-T, 31 March 2003.

ICTY, Final Report to the Prosecutor by the Committee Established to Review the NATO Bombing Campaign Against the Federal Republic of Yugoslavia.

Literature

Anthologies

Bailliet, Cecilia Marcela and Mujezinovic Larsen (ed.), *Promoting Peace Through International Law*. First edition, Oxford: Oxford University Press, 2015.

Besson, Samantha and Aspremont, Jean (ed.), *The Oxford Handbook on the Sources of International Law*. First edition, Oxford: Oxford University Press, 2017.

Casey-Maslen, Stuart (ed.), *Weapons under International Human Rights Law*. Cambridge: Cambridge University Press, 2014.

Cristiano, Fabio; Broeders, Dennis; Delerue, François; Douzet, Frederick and Géry, Aude (ed.), *Artificial Intelligence and International Conflict in Cyberspace*. Milton: Taylor & Francis Group, 2023.

[400] The preceding court of International Court of Justice (ICJ).

Deplano, Rossana and Tsagourias, Nicholas (ed.), *Research Methods in International Law: A Handbook*. Cheltenham/Northampton: Edward Elgar Publishing, 2021.

Fleck, Dieter (ed.), *The Handbook of International Humanitarian Law*. Fourth edition, Oxford: Oxford University, 2021.

Jonsson, Oscar (ed.), *Modern Warfare. New Technologies and Enduring Concepts*. Stockholm: Stockholm Free World Forum, 2020.

Krause, Maria and Scheinin (ed.), *International protection of human rights : a textbook*. Second edition, Turku/Åbo: Åbo Akademi University, 2012.

Moeckli, Daniel; Shah, Sangeeta and Sivakumaran, Sandesh (ed.), *International Human Rights Law*. Oxford: Oxford University Press, 2010.

White, Nigel D. and Henderson, Christian (ed.), *Research Handbook on International Conflict and Security Law. Jus ad Bellum, Jus in Bello and Jus Post Bellum*. Cheltenham/Northampton: Elgar Publishing, 2013.

Orford, Anne; Hoffman, Florian and Clark, Martin (ed.), *The Oxford Handbook of the Theory of International Law*. Oxford: University Press, 2016.

Saxon, Dan (ed.), *International Humanitarian Law and the Changing Technology of War*. International humanitarian law series, volume 41, Leiden/Boston: Martinus Nijhoff Publishers, 2013.

Shackelford, Scott J; Douzet, Frédérick and Ankersen, Christopher (ed.), *Cambridge:* Cambridge University Press, 2022.

Tsagourias, Nicholas and Buchan, Russell (ed.), *Research handbook on International Law and Cyberspace*. Cheltenham/Northampton: Edward Elgar Publishing, 2015.

Ziolkowski, Katharina (ed.) *Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy*. NATO Cooperative Cyber Defence Centre of Excellence (CCD COE Publication): Tallinn, 2013.

Book chapters

De Schutter, Olivier (2012), "The Status of Human Rights in International Law", in Krause, Maria and Scheinin (ed.), *International protection of human rights : a textbook*. Second edition, Turku/Åbo: Åbo Akademi University, 2012, pp. 39–58 [cit. "De Schutter, 2012"].

Chinkin, Christine (2010), "Sources", in Moeckli, Daniel; Shah, Sangeeta and Sivakumaran, Sandesh (ed.), *International Human Rights Law*. Oxford: Oxford University Press, 2010, pp. 103–123 [cit. "Chinkin, 2010"].

Fidler, David (2014), "Cyberattacks and international human rights law", in Casey-Maslen, Stuart (ed.), *Weapons under International Human Rights Law*. Cambridge: Cambridge University Press, 2014 [cit. "Fidler, 2014"].

Gill, Terry G. (2013), "Non-Intervention in the Cyber Context", in Ziolkowski, Katharina (ed.) *Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy*. NATO Cooperative Cyber Defence Centre of Excellence (CCD COE Publication): Tallinn, 2013 pp. 217–238 [cit. "Gill, 2013"].

Happold, Matthed (2013), “International humanitarian law and human rights law”, in White, Nigel D. and Henderson, Christian (ed.), *Research Handbook on International Conflict and Security Law. Jus ad Bellum, Jus in Bello and Jus Post Bellum*. Cheltenham/Northampton: Elgar Publishing, 2013.

Hayashi, Nobuo (2021), “General Principles of International Humanitarian Law”, in Fleck, Dieter (ed.), *The Handbook of International Humanitarian Law*. Fourth edition, Oxford: Oxford University, 2021, p. 81–92 [cit. “Hayashi, 2021”].

Joseph, Sara (2010), “Scope of application”, in Moeckli, Daniel; Shah, Sangeeta and Sivakumaran, Sandesh (ed.), *International Human Rights Law*. Oxford: Oxford University Press, 2010, pp. 150–170 [cit. “Joseph, 2010”].

Kammerhofer, Jörg (2016), “International Legal Positivism” in Orford, Anne; Hoffman, Florian and Clark, Martin (ed.), *The Oxford Handbook of the Theory of International Law*. Oxford: University Press, 2016, pp. 407–436 [cit. “Kammerhofer, 2016”].

Reisinger, H. and Golts A. (2014), “Russia’s Hybrid Warfare: Waging War Below the Radar of Traditional Collective Defence”, in *NATO Research Paper*, Research Division, NATO Defense College, Rome, No. 105, November 2014 [cit. “Reisinger och Golts, 2014”].

Sinclair, Sir Ian (1994), “The significance of the Friendly Relations Declaration”, in Lowe, Vaughan and Warbrick, Colin (ed.), *The United Nations and the Principles of International Law. Essays in memory of Michael Akehurst*. London: Routledge, 1994, pp. 1–32 [cit. “Sinclair, 1994”].

Schmitt, Michael (2015), “Introduction”, in Tsagourias, Nicholas and Buchan, Russell (ed.), *Research handbook on International Law and Cyberspace*. Cheltenham/Northampton: Edward Elgar Publishing, 2015 [cit. “Schmitt, 2015”].

Sivakumaran, Sandesh (2010), “International Humanitarian Law”, in Moeckli, Daniel; Shah, Sangeeta and Sivakumaran, Sandesh (ed.), *International Human Rights Law*. Oxford: Oxford University Press, 2010, pp. 522–539 [cit. “Sivakumaran, 2010”].

Sthoeger, Eran (2024), “Article 103 of the United Nations Charter: Uncharted Possibilities? The Ukraine Conflict and beyond”, in *Michigan Journal of International Law*. Vol. 45, no. 2, 2024, pp. [cit. “Sthoeger, 45 Mich. J. Int’l L., 2024”].

Summers, James (2013), “The internal and external aspects of self-determination reconsidered”, in French, Duncan (ed.), *Statehood and Self-Determination. Reconciling Tradition and Modernity in International Law*. Cambridge: University Press, 2013 [cit. “Summers, 2013”].

Wrange, Pål (2015), “Protecting Which Peace for Whom against What? A Conceptual Analysis of Collective Security”, in Bailliet, Cecilia Marcela and Mujezinovic Larsen (ed.), *Promoting Peace Through International Law*. First edition, Oxford: University Press, 2015 [cit. “Wrange, 2015”].

Books

Bailliet, Cecilia and Larsen, Kjetil Mujezinović, *Promoting peace through international law.* First edition, 2015 [cit. “Bailliet and Larsen, 2015”].

Boothby, William H., *The Law of Targeting*. Oxford: Oxford University Press, 2012 [cit. "Boothby, 2012"].

Bring, Ove; Klamberg, Mark; Mahmoudi, Said and Wrange, Paul, *Sverige och folkrätten*. Sixth edition, Stockholm: Norstedts Juridik, 2020 [cit. "Bring et al., 2020"].

Bring, Ove, *Anfallskrigens argument: konsten att rättfärdiga våld*. Lund: Historiska Media, 2022 [cit. "Bring, 2022"].

Byers, Michael, *War Law. International Law and Armed Conflict*. London: Atlantic Books, 2005 [cit. "Byers, 2005"].

Cambridge, James, *State responsibility: the general part*. First edition, Cambridge: University Press, 2013 [cit. "Cambridge, 2013"].

Clapham, Andrew, *Brierly's Law of Nations*. Seventh edition, Oxford: Oxford University Press, 2012 [cit. "Clapham, 2012"].

Coliver, Chloe; Pomerantsev, Peter; Applebaum, Anne and Birdwell, Jonathan, *Smearing Sweden*. London : ISD Global, 2018 [cit. "Coliver et al., 2018"].

Connable, Ben; Young, Stephanie; Pezard, Stephanie; Radin, Andrew; Cohen, Raphael S.; Migacheva, Katya and Sladden, James, *Russia's Hostile Measures: Combating Russian Gray Zone Aggression Against NATO in the Contact, Blunt, and Surge Layers of Competition.* Santa Monica, California: RAND Corporation, 2020, available via [https://www.rand.org/pubs/research_reports/RR2539.html#citation] [cit. "Connable et al, 2020"].

Crawford, James, *State Responsibility: The General Part*. First edition, Cambridge: Cambridge University Press, 2013 [cit. "Crawford, 2013"].

Crawford, James, *Brownlie's Principles of Public International Law*. Ninth edition, Oxford: University Press, 2019 [cit. "Crawford, 2019"].

Delerue, François, *Cyber Operations and International Law*. Cambridge: Cambridge University Press, 2020 [cit. "Delerue, 2020"].

Dinstein, Yoram, *The Conduct of Hostilities under the Law of International Armed Conflict*. Cambridge: University Press, 2004 [cit. "Dinstein, 2004"].

Distefano, Giovanni, *Fundamentals of Public International Law: A Sketch of the International Legal Order*. Leiden, Boston: Brill Nijhoff, 2019 [cit. "Distefano, 2019"].

Farrell, Michael, *Modern Just War Theory: A Guide to Research*. Lanham/Toronto/ Plymouth: The Scarecrow Press, 2013 [cit. "Farrell, 2013"].

Hill, Stephen M. Hill; Malik, Shahin P. and Croft, Stuart (ed.), *Peacekeeping and the United Nations*. Hants/Vermont: Dartmouth Publishing, 1996 [cit. "Hill et al., 1996"].

Henckaerts, Jean Marie and Doswald Beck, Louise, *Customary International Law. Volume I: Rules*. Cambridge: University Press, 2005 [cit. "Henckaerts and Doswald Beck, 2005, Vol. I"].

Henckaerts, Jean Marie and Doswald Beck, Louise, *Customary International Law. Volume II: Practice – Part 1*. Cambridge: University Press, 2005 [cit. "Henckaerts and Doswald Beck, 2005, Vol. II pt. 1"].

Henckaerts, Jean Marie and Doswald Beck, Louise, *Customary International Law. Volume II: Practice – Part 2*. Cambridge: University Press, 2005 [cit. "Henckaerts and Doswald Beck, 2005, Vol. II pt. 2"].

Henriksen, Anders, *International Law*. Oxford: Oxford University Press, 2017 [cit. "Henriksen, 2017"].

Keegan, John, *A History of Warfare*. London: Pimlico, 2004 [cit. "Keegan, 2004"].

Klabbers, Jan, *International Law*. Third edition, Cambridge: Cambridge University Press, 2021 [cit. "Klabbers, 2021"].

Kolb, Robert and Hyde, Richard, *An Introduction to International Law of Armed Conflict*. [cit. "Kolb and Hyde, 2008"].

Kolb, Robert, *An Introduction to the Law of the United Nations*. Portland: Hart Publishing, 2010 [cit. "Kolb, 2010"].

Linderfalk, Ulf; Nilsson, Anna; Sjöstedt, Britta and Wong, Kristoffer, *Folkrätten i ett nötskal*. Third edition, Lund: Studentlitteratur, 2020 [cit. "Linderfalk et al., 2020"].

McCorquodale, Robert and Dixon Martin, *Cases and materials on international law*. Fourth edition, Oxford: Oxford University Press, 2003 [cit. "McCorquodale and Dixon, 2003"].

Melzer, Nils, *International Humanitarian Law – A Comprehensive Introduction*. Geneva: International Committee of the Red Cross, 2022 [cit. "Melzer, 2022"].

Merkouris, Panos, *Article 31(3)(c) VCLT and the Principle of Systemic Integration. Normative Shadows in Plato's Cave*. Queen Mary studies in international law, vol. 17, 2015 [cit. Merkouris, 2015].

Newton, Michael and May, Larry, *Proportionality in International Law*. Oxford: University Press, 2014 [cit. "Newton and May, 2014"].

Ramberg, Christina; Besher, Alexander R.; Carlson, Laura; Croon, Adam; Granmar, Claes; Kleist, David; Leviner, Pernilla and Norée, Annika, *Rättskällor – en introduktion i kritiskt tänkande*. Second edition, Stockholm: Norstedts Juridik, 2024 [cit. "Ramberg et al., 2024"].

Snyder, Timothy, *Bloodlands: Europe Between Hitler and Stalin*. New York: Basic Books, 2010 [cit. "Snyder, 2010"].

Solis, Gary D., *The Law of Armed Conflict. International Humanitarian Law in War*. Third edition, Cambridge: Cambridge University Press, 2022 [cit. "Solis, 2022"].

Svanberg, Katinka, *En introduktion till traktaträtten. En lärobok i traktaträtt*. Fifth edition, Stockholm: Norstedts juridik, 2015 [cit. "Svanberg, 2015"].

Svanberg, Katinka and Bring, Ove, *FN-stadgan och världspolitiken*. Fifth edition, Stockholm: Norstedts Juridik, 2019 [cit. "Svanberg and Bring, 2019"].

Thürer, Daniel, *International Humanitarian Law: Theory, Practice, Context*. Hague Academy of International Law, 2011 [cit. “Thürer, 2011”].

Wacks, Raymond, *Understanding Jurisprudence*. Sixth edition, Oxford: Oxford University Press, 2021 [cit. “Wacks, 2021”].

Weissbrodt, David and de la Vega, Connie, *International Human Rights Law: An Introduction*. Philadelphia: University of Pennsylvania Press, 2007 [cit. “Weissbrodt and de la Vega, 2007”].

Winther, Pontus, *International Humanitarian Law and Influence Operations. The Protection of Civilians from Unlawful Communication Influence Activities during Armed Conflict*. Uppsala: Acta Universitatis Upsaliensis, 2019 [cit. “Winther, 2019”].

International Red Cross Committee Commentaries

International Red Committee, *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 [cit. “ICRC Commentary on AP I, 8 June 1987”].

Melzer, Nils, *Interpretative Guidance on the Direct Participation in Hostilities under International Humanitarian Law*. ICRC, 2009.

Periodical journals

Buchan, Russell (2013), “Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?”, in *Journal of Conflict & Security Law*. Oxford: Oxford University Press, 2012 [cit. “Buchan, 2013”].

D’Amato, Anthony (2010), “Is International Law Part of Natural Law?”, in *Northwestern University School of Law, Faculty Working Papers*, paper 68 [cit. “D’Amato, 2010”].

Doswald–Beck, Louise and Vité, Sylvain (1993), “International Humanitarian Law and Human Rights Law”, in *International Review of the Red Cross*. 1993/04, Vol. 33 (293), p. 94–119, 1993 [cit. “Doswald-Beck and Vité, 1993”].

Eide, Asbjørn; Rosas, Allan; Meron, Theodor (1995), “Combating Lawlessness in Gray Zone Conflicts Through Minimum Humanitarian Standards", in *The American Journal of International Law*. 1995-01, Vol. 89(1), p. 215–223 [cit. “Eide et al., 1995”].

Hollis, Duncan B. (2007), "Why States Need an International Law for Information Operations", in *Lewis & Clark Law Review*. Vol. 11, p. 1023–1061, 2007 [cit. “Hollis, 2007”].

Fogt, Morten M. (2020), "Legal Challenges or 'Gaps' by Countering Hybrid Warfare – Building Resilience in Jus Ante Bellum", in *Southwestern Journal of International Law*. Vol. VII:1, 2020, s. 28–100 [cit. “Fogt, 2020”].

Jordan, Thomas P., “The Law of Armed Conflict, Unconventional Warfare, and Cyber Attacks”, in *American University National Security Law Brief*. Vol. 6, No. 2, 2016, pp. 37–58 [cit. “Jordan, 2016”].

Katz, Eian (2020), “Liar’s war: Protecting civilians from disinformation during armed conflict”, in *International Review of the Red Cross*. Vol. 102(914), pp. 659–682 [cit. “Katz, 2020”].

Linderfalk, Ulf (2011), “International Legal Hierarchy Revisited: The Status of Obligations Erga Omnes”, in *Nordic Journal of International Law*, Vol. 80, 2011, pp. 1–23 [cit. “Linderfalk, 2011”].

Locomotive Engineers Journal, February 1929.

Margulies, Peter (2013), “Sovereignty and Cyber Attacks: Technology’s Challenge to the Law of State Responsibility”, in *Melbourne Journal of International Law.* [cit. “Margulies, 2013”].

Peperkamp, L. (2016), “The Blurry Boundaries Between War and Peace. Do We Need to Extend Just War Theory?”, in *Archiv für Rechts- und Sozialphilosophie.* 102/3, pp. 315–332 [cit. “Peperkamp, 2016"].

Tsagourias, Nicholas (2012), “Cyber attacks, self-defense and the problem of attribution”, in *Journal of Conflict & Security Law*. Vol. 17, No. 2 (2012), pp. 229–244 [cit. “Tsagourias, 2012”].

Wallace Brown, Garrett and Bohm, Alexandra (2016), “Introducing Jus Ante Bellum as a cosmopolitan approach to humanitarian intervention”, in *European Journal of International Relations*. Vol 22(4), pp. 897–919 [cit. “Wallace Brown and Bohm, 2016”].

Wheatley, Steven (2020), “Foreign Interference in Elections Under the Non-Intervention Principle: We Need to Talk About ‘Coercion’”, in *Duke Journal of Comparative & International Law*. Vol. 31:161, 2020 [cit. “Wheatley, 2020”].

Internet sources

Aftonbladet, “Natotoppens oro: Varnar för rysk hybridattack med många döda”, 2024-12-29, available via [https://www.aftonbladet.se/nyheter/a/zAQdLb/natotoppens-oro-varnar-for-rysk-hybridattack-med-manga-doda], accessed 2024-12-29.

America’s Cyber Defense Agency, “Cyber-Attack Against Ukrainian Critical Infrastructure”, available via [https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01], accessed 2024-10-15.

CCPR Centre, “Article 20: Prohibition of propaganda for War and Advocacy of National, Racial or Religious Hatred”, in *Simple Guide on The International Covenant on Civil and Political Rights (ICCPR)*. Available via [https://ccprcentre.org/files/media/ICCPR_easy_to_read_commentary_WEB.pdf], accessed 2024-12-29.

Djinis, Elizabeth (2017), “How will cyber warfare change the future? Jared Cohen has some ideas” in Herald-Tribune, available via [https://eu.heraldtribune.com/story/news/local/sarasota/2017/02/20/how-will-cyber-warfare-change-future-jared-cohen-has-some-ideas/22424667007/], accessed 2024-10-24.

Expressen, “Ryska hybridhotet mot Nato: ‘En kokande groda’”. 2025-01-01, available via [https://www.expressen.se/nyheter/varlden/ryska-hybridhotet-mot-nato-kokande-groda/], accessed 2025-01-01.

General Comment No. 11 of the HR Committee (HRI/GEN/1/Rev.9 [Vol. I] p. 182), particularly § 2. Available via [http://ccprcentre.org/ccpr-general-comments], accessed 2024-12-29.

ICRC, Advisory Service on International Humanitarian Law, *International Humanitarian Law and International Human Rights Law: Similarities and differences*, available via [https://www.icrc.org/sites/default/files/document/file_list/ihl-and-ihrl.pdf], accessed 2024-11-22.

ICRC CIHL Study, *Customary International Humanitarian Law Database*. Available via [https://ihl-databases.icrc.org/en/customary-ihl/] [cit. "ICRC CIHL Study"].

ICS Alert, "Cyber-Attack Against Ukrainian Critical Infrastructure", (last revised 20 July 2021), available via [https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01], accessed 2025-01-03.

Kim, Young Mie (2020), "New Evidence Shows How Russia's Election Interference Has Gotten More Brazen", Brennan Center for Justice, 2020-03-05, available via [https://www.brennancenter.org/our-work/analysis-opinion/new-evidence-shows-how-russias-election-interference-has-gotten-more], accessed 2024-10-14.

NBC News, "TikTok says it's not spreading Chinese propaganda. The U.S. says there's a real risk. What's the truth?". 2024-09-16, available via [https://www.nbcnews.com/investigations/tiktok-says-not-spreading-chinese-propaganda-us-says-real-risk-rcna171201], accessed 2024-09-29.

North Atlantic Treaty Organization (NATO), *Statement by the North Atlantic Council on recent Russian hybrid activities.* Published 2024-05-04, available via [https://www.nato.int/cps/en/natohq/official_ texts_225230.htm?selectedLocale=en], accessed 2024-05-03.

Oxford Reference, *Erga omnes obligations*, available via [https://www.oxfordreference. com/display/10.1093/oi/ authority.20110803095756413], accessed 2024-10-13.

Reuters, "Putin draws a nuclear red line for the West", 2024-09-27, available via [https://www.reuters.com/world/europe/putin-draws-nuclear-red-line-west-2024-09-27/], accessed 2025-01-03.

South Southwest PTTC, "Measuring an Ounce of Prevention and a Pound of Cure", available via [https://pttcnetwork.org/measuring-an-ounce-of-prevention-and-a-pound-of-cure/#:~:text=%E2%80%9CAn%20ounce%20of%20prevention%20is,%E2%80%9D%20and%20the%20%E2%80%9Cpound.%E2%80%9D].

The Guardian, *Russia–Ukraine crisis: Putin orders military operation in Ukraine*. Available via [https://www.youtube.com/watch?v=asuhx16wlWo], accessed 2024-03-07.

The Guardian, "How did Donald Trump end up posting Taylor Swift deepfakes? AI images posted to Truth Social bore the watermark of a tiny Texas non-profit looking to bankroll X users". 2024-08-26, available via [https://www.theguardian.com/technology/article/2024/aug/24/trump- taylor-swift-deepfakes-ai], accessed 2024-10-07.

The White House, "International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World", May 2011 [https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_ for_cyberspace.pdf], accessed 2024-11-22.

Wired, “Russian Propaganda Unit appears to Be Behind Spread of False Tim Walz Sexual Abuse Claims. The Russian-aligned network Storm-1516 has a long history of posting fake whistleblower videos—including deepfakes—to push Kremlin talking points”, 2024-10-21, available via [https://www.wired.com/story/russian-propaganda-unit-storm-1516-false-tim-walz-sexual-abuse-claims/], accessed 2024-10-22.

World Risk Poll (Gallup), “’Fake news’ is the number one worry for internet users worldwide”, 2020-06-10, available via [https://wrp.lrfoundation.org.uk/news/fake-news-is-the-number-one-worry-for-internet-users-worldwide], accessed 2024-11-15.

Consulted reference literature

Evans, Malcolm D., *Blackstone’s International Law Documents*. Sixteenth edition, Oxford: Oxford University Press, 2024.

Mahmoudi, Said, *Folkrättsliga texter*. Fifth edition, Stockholm: Norstedts Juridik, 2021.

Oxford Standard for Citation of Legal Authorities (OSCOLA), *Citing International Law Sources Section*. University of Oxford: Faculty of Law, 2006, available via [https://www.law.ox.ac.uk/sites/default/files/migrated/oscola_2006_citing_international_law.pdf].