INTERNET POLICY REVIEW
Journal on internet regulation

Volume 9 | Issue 3

Public and private just wars: Distributed cyber deterrence based on Vitoria and Grotius

Johannes Thumfart
Law, Science, Technology and Society, Vrije Universiteit Brussel, Belgium,
Johannes.Thumfart@vub.be

Published on 16 Sep 2020 | DOI: 10.14763/2020.3.1500

Abstract: This contribution discusses the growing importance of cyber attacks directed at the public sphere and the crucial role of non-state actors in cyber attacks from a perspective of just war theory. Going back to Grotius' and Vitoria's seminal teachings on international law, the article makes the case for distributed cyber deterrence involving private and public actors. Further, it justifies sanctions for cyber attacks that do not cause physical violence, for example the interference with elections or the hacking of companies. It considers the post-physicality of cyberspace, the attribution problem, private just war theory and national self-determination through deliberation.

Keywords: Cyber attacks, Cyber deterrence, Just war, Active Cyber Defense Certainty Act, Active cyber defense, Grotius, Vitoria, Tallinn Manual

Article information

Received: 26 Sep 2019 **Reviewed:** 20 Dec 2019 **Published:** 16 Sep 2020

Competing interests: The author has declared that no competing interests exist that have influenced the text.

URL:
http://policyreview.info/articles/analysis/public-and-private-just-wars-distributed-cyber-deterrence-based-vitoria-and

Citation: Thumfart, J. (2020). Public and private just wars: Distributed cyber deterrence based on Vitoria and Grotius. *Internet Policy Review*, *9*(3). DOI: 10.14763/2020.3.1500

This paper is part of Geopolitics, jurisdiction and surveillance, a special issue of Internet Policy Review *guest-edited by Monique Mann and Angela Daly.*

INTRODUCTION

There is a growing tendency to apply just war theory to cyberspace (e.g., Finlay, 2018; Smith, 2018; Sleat, 2017; Thumfart, 2017; Smotherman, 2016; Giesen, 2014; Solis, 2014; Taddeo, 2014). This corresponds to three developments at the intersection of international relations and digital studies.

First: just war theory drafts a way in which individual states can secure international peace. It is therefore compatible with the declining relevance of traditional institutions of global governance and the emergence of a multi-polar world order.

Second: since they are not directly connected to military losses, relatively cheap to execute and difficult to attribute, cyber warfare and cyber attacks encourage offensive strategies (Taddeo 2018a, p. 324; Lin, 2012, p. 521). When peace cannot be guaranteed through supremacy of defense, it has to be secured through deterrence. And since "deterrence means dissuading someone from doing something by making them believe that the costs to them will exceed their expected benefit" (Nye, 2017, p. 45), it depends on credibility (McKenzie, 2017, p. 2). Credibility, in turn, is achieved by formalisation and legitimisation of sanctions such as offered by just war theory.

Third: just war theory might appear archaic. And correctly so. After all, it is an ethical, so to speak: proto-legal, concept. It should compensate for the *absence* of reliable legal standards. Although it is a broad consensus that international law and the UN Charter in general apply to cyberspace, there is still no specific international legal framework concerning cyber attacks.

This lack of legal framework or even basic orientation primarily concerns *jus ad bellum,* i.e. the question of when a state has the right to retaliate cyber attacks proportionately.

The Tallinn Manual 2.0, which is issued by NATO to clarify the application of international law to cyber attacks, is explicitly undecided on the matter. On the one hand, it generally states that "the right to employ force in self-defence extends beyond kinetic armed attacks to those that are perpetrated solely through cyber operations." And it expresses a broad consensus by stating that a "cyber operation that seriously injures or kills a number of persons or that causes significant damage to, or destruction of, property would satisfy the scale and effects requirement" (Schmitt and NATO, 2017, p. 340).

On the other hand, the manual expresses significant uncertainty concerning cyber aggressions without direct physical consequences, such as the manipulation of elections, stock markets or deliberative processes in the public sphere. "The case of cyber operations that do not result in injury, death, damage, or destruction, but that otherwise have extensive negative effects, remains unsettled" (Schmitt and NATO, 2017, p. 340f.).

Likewise, in 2018, the US State Department called for a "fundamental rethinking" of "strategies for deterring malicious cyber activities" (State Department, 2018). But it failed to clarify, too, which attack would trigger what response – a quite remarkable silence on this issue, since, just recently, one of the world's oldest and still most powerful democracies became a victim of Russian cyber operations interfering with its public sphere (Matishak, 2018).

Next to the *jus ad bellum* of states, cyber attacks are atypical from a Westphalian perspective because they directly involve private actors. Not just as aggressors, i.e. as independent hacker groups or state-sponsored proxies, but also as its primary victims.

Concerning private actors, too, the right of reprisals, i.e. "hack-back" and "active cyber defense", has been debated, for example in the context of the proposed Active Cyber Defense Certainty Act discussed in US congress. This is all the more urgent because in cyberspace "the top tech companies appear to be as powerful as States, and sometimes even more so, to prevent cyber attacks, attribute them and to respond to malicious acts" (Bannelier and Christakis, 2017, p. 10; see also Gstrein, 2020, in this issue). And Facebook and Google have already engaged in active

cyber defense without having been prosecuted by the US government (Glosson, 2015, p. 17; Huang, 2014, p. 1234).

Nevertheless, the Tallinn Manual unambiguously reads: "Only States may take countermeasures. For example, an information technology firm may not act on its own initiative in responding to a harmful cyber operation" (Schmitt and NATO, 2017, p. 130).

This contribution represents a realistic approach to cyber deterrence inasmuch as it focuses on two essential features that are usually omitted in the debate about just cyberwar and can be considered elephants in the room: public wars and private wars.

First, *public wars:* whilst the philosophically intriguing question of the physicality of cyber attacks still dominates theory, there seems to be a broad consensus in practice that it is irrelevant as long as cyber attacks have *effects that are physically violent*, such as this is expressed in the Tallinn Manual 2.0 quoted above. A clear expression of this virtually global consensus is that cyber attacks with physically violent effects are extremely rare, also beyond NATO states. Due to their unclear legal status much more attractive and frequent are cyber aggressions aimed at manipulating deliberative processes in the public sphere. They are therefore a much more urgent object of a theory of just cyberwar.

Due to these questions, in section 1, I will go back to the origin of modern just war theory and international law, to Francisco de Vitoria, who developed a framework of international law that understands communication as the highest normative value. Contrary to contemporary misconceptions of just war theory (Taddeo, 2014, p. 7), Vitoria's original doctrine did not focus on the physicality of the means or the effects of an attack as *casus belli*, but rather on the gravity of the violation of rights connected to an attack, especially in regard to communication, which makes his theory interesting to contemporary problems.

In this context, I will also discuss Vitoria's early answer to the attribution problem in section 2: the conduct of coercion-free and transparent multi-stakeholder discourses that minimise the risk of false attribution, which resembles the contemporary demand to constitute an independent global institution responsible for attributing cyber attacks (Davis et al., 2017).

In section 3, I will show how Vitoria's concept of *ius communicationis,* the "right to communicate", allows for proportionate sanctions of cyber attacks directed at the public sphere.

The second focus of this contribution lies on the question of *private wars*. The debate concerning just cyberwars so far omits the role of private actors. Not so the classics. In his earliest writing on international law, Grotius coined the term *bellum iustum privatum,* private just war. How companies could justify hack-back and active cyber defense relating to this concept will be discussed in section 4.

If one accepts the right of companies to actively defend themselves in cyberspace, then one must also pose the question of how individual citizens could legitimately and actively defend their human right to privacy against intrusive state actors and companies[1]. To a realistic long-term perspective of deterrence, a medially and digitally literate, critical, and in extreme cases, actively disobedient civil society poses no threat, but, on the contrary, states should encourage such "civilian-based deterrence" (Thumfart, 2011; Sharp, 1985). Private and public cyber deterrence capacities together make up a system of distributed deterrence that is much more realistic, effective and secure than state-based deterrence alone and makes "the proverbial square peg" of cyber deterrence fit into the "round hole" of deterrence theory (Taddeo, 2018a, p. 325).

SECTION 1: WHAT CONSTITUTES AN ATTACK? A CONSTRUCTIVIST APPROACH BEYOND THE CYBERSPACE PHYSICALITY PROBLEM

Vitoria's lectures are broadly recognised as the first teachings on international law and the first modern account of just war theory. His just war doctrine immediately leads to the question of physicality. Echoing the classical doctrine of *vim vi repellere licet*, Vitoria says: "There can be no doubt about the rights of defensive war, since it is lawful to resist force with force" (Vitoria, 1991, p. 297).

This long-lived tradition is also echoed by Article 51 of the UN Charter, which claims an "inherent right of collective or individual self-defense" as part of natural law that has to be understood as an exception to the positive norm of the prohibition of the use of armed force in article 2 (4) (Christakis and Bannelier, 2017, p. 36).

Before the digital age, it would have been unnecessary to stress that "force" (Latin: *vis*) is a physical term. The physicality of cyberspace, in turn, is a heavily debated issue. Insisting on the mere virtuality of cyberspace in order to exempt it from the physical scope of law in general has been a common trope in the debate from its beginning on, leading to conservatives' fear of "cyber anarchy" (Goldsmith, 1999).

However, cyberspace is of course, in fact, based on physical infrastructure. And it is of course wrong to state that "cyber attacks are nonphysical" (Smith, 2018, p. 222) or that they mark a "shift toward the non-physical domain" (Taddeo 2012, p. 106). It has for example been argued that data has a (however minimal) weight (Ray, 2011; Robinson, 2018). And it has been acknowledged in criminal law that the obtaining of e-evidence from servers abroad constitutes a physical intrusion in a different jurisdiction. "Contrary to the current metaphor often used by Internet-based service providers, digital information is not actually stored in clouds; it resides on a computer or some other form of electronic media that has a physical location" (In re Warrant to Search Target Computer at Premises Unknown. 958 F. Supp. 2d 753, S.D. Tex, 2013).

Nevertheless, for a long time, the dominant interpretation of the UN Charter's prohibition of the use of "force" in Article 2(4) applied this prohibition only to kinetic, i.e. non-digital attacks (Waxman, 2011, p. 45). As Orend puts it: "The gold standard of *casus belli* is a kinetic physical attack" (Orend, 2013, p. 176).

However, it is clear that cyber attacks, for instance attacks on transportation infrastructure or on factories, can have physical consequences. Take the Stuxnet attack: it could be considered a kinetic attack. Although it was primarily executed by non-kinetic means, it had kinetic consequences (Jenkins, 2013, p. 70). Therefore, a new consensus emerged that no longer focuses on the *physicality of the means*, but, rather, on the *physically violent effects* of an attack.

The Tallinn Manual 2.0 seems to express this latest consensus in its rule 69. "A cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force" (Schmitt and NATO, 2017, p. 330). This seems to leave the issue of attacks that produce *effects that are not physically violent*. "The case of cyber

operations that do not result in injury, death, damage, or destruction, but that otherwise have extensive negative effects, remains unsettled" (Ibid., p. 342).

In another passage, however, the Tallinn Manual indicates that its authors do not understand the term "injury" in a physical way. "The term 'injury' is not to be understood to require damage. Instead, simple breach of an international legal obligation suffices to make proportionate countermeasures available to the injured State" (Ibid., p. 127).

In addition to the criteria of the physicality or non-physicality of means or effects, in the Tallinn Manual, it is the criteria of *coerciveness* that is decisive regarding whether an action can be met with countermeasures. "The fact that cyber operations result in no physical consequences does not detract from their characterisation as a prohibited intervention. By way of contrast, a cyber operation that does not seek any change of conduct lacks the requisite coercive element" (Ibid., p. 318).

This of course raises the question of how to determine the coerciveness of an action. What is coercive to a small nation hardly affects a powerful nation. Or, is the criteria of coerciveness only fulfilled if an explicit threat has been formulated? Something along the lines: "we did A to you, so that you do B"? The criteria of coerciveness will be dealt with again later on (sections 2 and 3).

As Russia's various interventions around the US elections in 2016 have shown (Matishak, 2018), the unclarity regarding the criteria that are needed to justify countermeasures led to a reality, in which attacks on the public sphere remain unsanctioned. This is because they cannot be easily placed within these three categories: physically violent means, physically violent effects or coerciveness. Similar attacks targeting elections, the freedom of the press or financial markets are plausible and must seem attractive to aggressors. Deterrence-oriented just war theory must find an answer to this problem.

For this undertaking, it is helpful to take a step back to the origins of modern just war doctrine in Vitoria's lectures. Next to the physicalism characteristic to Roman Law and its *vim vi repellere licet* discussed above, his theory focuses on the effects that actions have on people's rights, not just the physical means or effects of an attack.

This needs to be uncovered with the help of the original Latin text of Vitoria's lectures. In the standard English translation, he clarifies the *jus ad bellum* as self-defense with the following words: "The sole and only just cause for waging war is when harm has been inflicted" (Vitoria, 1991, p. 303).

The word "harm" seems to indicate physicality. In the Latin original, however, it says *iniuria*, which is far better translated with "injustice" than with "harm", as this is the case in the German translation, which uses the term "*Unrecht*", i.e. "injustice" (Vitoria, 1997, p. 558). In fact, in a decisive paragraph discussed below, also the English translation uses the more adequate term "offence" for *iniuria* (section 3).

In short: decisive to the legitimacy of just war is not the gravity of the action or its effects, but the gravity of the violation of a subject's natural rights. We will later see that, due to this definition, Vitoria's doctrine allows for sanctions to actions that do not include physical violence (section 3).

This whole problem becomes clearer with some philosophical remarks. Of course, the is-/ought-

distinction would have been completely alien to a natural rights lawyer such as Vitoria. However, in terms of contemporary philosophy, it makes sense to apply it.

The physicality problem in the just cyberwar debate might be overall the wrong question to ask. It is yet another is-ought-fallacy that characterises many positions in the debate about cyberspace, which continue deducing normative claims from a supposed "nature" of cyberspace, preferably along the equation: non-physical = without legal consequences (De Hert and Thumfart, 2018, p. 5).

This necessity to separate normative and descriptive claims has been, in part, understood by Jenkins who denies that the physicality or non-physicality of the means used for an attack makes a "morally relevant difference" (Jenkins, 2013, p. 74). Similarly, Sleat dismisses the debate around the physicality of means by pointing out that just war theories ultimately concern "specific human actions and their effects on a particular group of other human beings", and that, therefore, they must ultimately address this "human question", i.e. categories that are rather relevant to normative discourses than to descriptive ones: the impact of aggressions "on our projects and purposes" (Sleat, 2017, p. 333).

At Vitoria, the ultimate irrelevance of the question of physicality to just war is grounded in a thick communitarian ontology and anthropology, which he inherited from Aristotle and Aquinas. Vitoria takes the Aristotelian dictum that humans are political animals, quite literal, inasmuch as he insists that a human being outside of the political community is not human, but an animal (Vitoria, 1995, p. 125).

This communitarian anthropology also offers a radically minimal, anachronistically speaking constructivist solution to the metaphysical problem of the existence of physicality independent from human beings. Even if there was "wisdom without speech" (*sapientia* [...] *sine sermone*), Vitoria says, such truth would be of no value because it would be "unedifying and unsociable" (*ingrata et insociabilis esset ipsa sapientia*) (Vitoria, 1995, p. 123).

In this sense, the question of physicality is not decisive. Rather, the issue has to be, whether the existence of an object is communicated or not. In the same way, contemporaries concluded that the issue of just cyberwar calls for a "constructivist approach to cyber deterrence emphasizing intersubjective understandings" (Lupovici, 2016, p. 328). A constructivist approach is an approach that does not conceive of empirical reality as something given independently from human discourse, but rather, as something being *constructed* by a discourse. Such an approach is especially useful in order to address the problem of how to determine and assess coerciveness, which will be dealt with in sections 2 and 3.

A constructivist approach based on Vitoria's original just war theory also solves the problem of the perception of an "ontological gap between just war theory and cyber conflicts" (Taddeo, 2018b, p. 350), which seems to be owed to a two-fold misconception: the misconception of cyberspace as non-physical (Taddeo 2012, p. 106) and the simplification of just war theory as being "centered on human beings, tangible objects, and kinetic conflicts causing physical damage and bloodshed" (Taddeo, 2018b, p. 350).

However, there are, of course, grave difficulties with such an intersubjective and constructivist approach. Due to its epistemological openness, such a broad understanding of *casus belli* could easily turn into a *carte blanche* for military aggression.

SECTION 2: THE ATTRIBUTION PROBLEM: TRANSPARENT DISCOURSE INSTEAD OF *CARTE BLANCHE*

Whether an intersubjective understanding of *casus belli* becomes a dangerous *carte blanche* for military aggression or an effective means of cyber deterrence largely depends on solving the attribution problem.

It is surely exaggerated and not consistent to state that in cyberspace "attribution is at best problematic, if not impossible" and to deny the possibility of cyber deterrence on these grounds (Taddeo, 2018b). This can be easily shown by employing the domestic analogy from Walzer's just war theory: this would be as if one argued for an end to law enforcement activities against cybercrime because it is hard to catch cybercriminals.

In general, however, it is indeed difficult to attribute cyber attacks, due to the involvement of non-state hacker groups acting as proxies or autonomously, various degrees of anonymity on the web, the widespread practice of staging false flag attacks (Skopik and Pahi, 2020), such as happened during the 2018 Olympics cyber attack (Greenberg, 2019b) and difficulties regarding the obtaining of extraterritorial e-evidence. Those difficulties are not only responsible for the fact that, so far, there is no standard procedure for attributing cyber attacks, but also for the fact that they are rarely officially attributed by and to states at all.

In order not to get carried away by the endless possibilities of theory, it is important to provide three examples of attribution in practice.

1. *The distributed denial-of-service attack (DDoS-attack) on Estonia in 2007*: In the context of a heated debate around the relocation of Russian war memorials, websites of Estonian media companies, banks and government agencies were flooded with superfluous requests by bots and individuals. This overload caused a collapse of systems.

In the realm of the grand, but often empty gestures of symbolic politics, the incident led to the instalment of the NATO Cooperative Cyber Defence Centre in the Estonian capital (McGuinness, 2017). This clearly invoked the idea of a new cold war in cyberspace. In reality, however, the seemingly clear front between the two blocks of yore was in fact a blurry line.

Since the criminal investigation of the attacks showed that the majority of the attackers could be located within the Russian jurisdiction, the Estonian Public Prosecutor issued a formal investigation assistance request to Russia. Russia, in turn, after first ensuring assistance, eventually denied it by arguing that it was not covered by the Mutual Legal Assistance Treaty (Tikk and Kaska, 2010). It blamed the attack on the pro-Kremlin youth movement *Nashi*, who took responsibility and stressed the autonomy of its actions (Shachtman, 2009). So far, the only person who has been tried for the attack was the Estonian citizen Dmitri Galushkevich, part of the country's large Russian ethnic minority. He was fined 17,500 Estonian Krooni, which roughly amounts to US$ 1,600 dollars (BBC, 2008).

2. *North Korea's attacks on Sony in 2014*: Due to North Korea's indignation about the then-upcoming comedy *The Interview*, which included a plot to assassinate Kim Jong-un, the North Korean hacker group *Guardians of Peace* hacked Sony's computer network, demanded the withdrawal of the movie and leaked confidential information. This led to the resignation of a

high-ranking Sony employee, among other effects. Primarily as a reaction to cinema chains' fear of making themselves the target of cyber attacks by getting involved, Sony decided to pull the theatrical premiere.

However, on 19 December, the FBI announced the attribution of the attack to North Korea, primarily because some of the tools used were similar to tools used before in attacks on South Korea. The very same day, the former US president Obama announced a proportionate response to North Korea and insisted on the release of the movie. Sony subsequently released the movie online and in some cinemas without suffering further attacks. It is unclear whether the US' response went further than imposing additional economic sanctions. In 2016, a private sector investigation made the evidence of the attribution available to the public (Novetta, 2016).

3. *The Democratic National Committee (DNC) hacking on the eve of the 2016 elections*: this was the first attack that was officially recognised as a confrontation between the two superpowers Russia and the US. Whilst the FBI contacted the DNC as early as September 2015 with a warning that their systems had been accessed by hackers linked to Russian intelligence, it took the DNC six months to hire a private security firm in order to protect their systems. The internal emails obtained in the attack were released by WikiLeaks from 22 July up to the election, causing the resignation of high-ranking DNC officials and influencing the US elections to an unclear extent.

In spite of Guccifer 2.0, the fictional persona crafted by Russian intelligence, causing the desired confusion, the early attribution to Russia was soon publicly confirmed by several cyber experts and private security firms and narrowed down to Russia's secret service (Banks 2017, p. 1488). Roughly a month before the election, the Department of Homeland Security (DHS) and the Office of the Director of National Intelligence (ODNI) published a joint statement that the Intelligence Community was confident that the Russian government was responsible for the attack and that it signified, indeed, an attempt to "interfere with the US election process" (DHS and ODNI, 2016). During that time, Obama reportedly exhorted Putin on the so called red phone that "international law, including the law for armed conflict, applies to actions in cyberspace" (Arkin, 2016).

Nevertheless, it took until January 2017, two months after the elections, until the public was provided with access to a declassified version of a report that contained some of the evidence supporting the attribution to Russia (ODNI, 2017). Somewhat ironically, before the elections, it was exactly the fear that the hack would strongly influence the elections, which prevented the Obama administration from acting faster. Another reason was, of course, that it needed to be absolutely sure not to unnecessarily escalate the conflict between the two superpowers with an unjustified public attribution. Additionally, a great part of the evidence was obtained by intelligence activities and not considered suitable for the critical eyes of the public.

These examples show four essential features of the attribution of cyber attacks:

1. *A long lag time between attack and attribution makes deterrence difficult*. As Banks points out concerning the DNC hacks, countermeasures should be immediate, because they "are designed to persuade the perpetrator to stop its unlawful actions, not as punishment or escalation"; and, therefore, a too long lag time between hack and attribution will turn legal active self-defense into unilateral punishment illegal under international law (Banks, 2017, p. 1502).
2. *The more unclear the attribution the more effective the attack*. Difficulties in attribution are the worst effect of attacks on the public sphere. Whilst North Korea wanted the US to know who committed the attack, and its attack therefore had no grave effects, the case is different

with the Russian DNC hacks and even *Nashi*'s in other ways extremely unsophisticated attacks on Estonia, which directly aimed at undermining trust in public deliberation, respectively instrumentalised existing ethnic conflicts within Estonia.
3. *The attribution problem is no preliminary problem to effective deterrence*, as it may seem, but, since undermining trust in public discourse is the main target of many cyber attacks, solving the attribution problem is already part of an effective defense strategy.
4. *The lack of explicit coerciveness makes the attack more effective*. In spite of having devastating effects, causing chaos and the erosion of trust in deliberative processes, attacks on the public sphere cannot be understood from a coercion-centred approach. On the contrary, such attacks are precisely characterised by their lack of an explicit threat structure. Explicit coerciveness causes less confusion and, due to providing a clear concept of the enemy, can even reinforce the trust in the attacked nation's institutions and deliberative processes.

It is interesting that already Vitoria, who lived in a time with less possibilities to verify the occurrence of an attack, saw the problem that the existence of a cause for just war might not be evident. Concerning this problem, he seems to foreshadow Kant's principle of publicity (Thumfart, 2013) by demanding that there must be a public, objective and balanced discussion free from coercion that includes representatives of the opposing nation and experts:

> For the just war it is necessary to examine the justice and causes of just war with great care, and also to listen to the arguments of the opponents, if they are prepared to negotiate genuinely and fairly. One must consult reliable and wise men who can speak with freedom and without anger or hate or greed (Vitoria 1991, p. 307).

One should not hold Vitoria's historical sexism against him, who only speaks of "men" (*viros*) here. And of course, a realist might add, such a public discussion including the opponent would render a military reprisal practically impossible. But maybe that is exactly what Vitoria intended, since he repeatedly asserts that just war must be a last resort. And this surely must also be the starting point for every not war-mongering, and hence reasonable just war theory.

On the other hand, public discourse concerning cyber attacks with public access to the available evidence seems to be a useful means to solve the dilemma of the attribution of cyber attacks, which consists in either carrying out a response too soon and wrongly attributed or not responding at all, because it is too late. In addition to that, an early public debate has the potential to prevent the erosion of trust in national deliberative processes, which is the strategic target of cyber attacks on the public sphere.

A practical problem here is that a primary means by which nation states can achieve accurate attribution is that they have information collected through espionage. This may enable those states to have confidence in attributions, but they will be extremely reluctant to reveal all the evidence behind such attributions in a timely manner to the public. In the specific case of the DNC hack, the attribution to Russia was apparently in substantive part due to the Russian hacking operation being hacked by Dutch intelligence (Gallagher, 2018).

An independent, albeit not public discussion of evidence of *casus belli* is supported by a paper of Rand Corporation on the matter, which mentions some factors for establishing credible attribution: the inclusion of independent experts, the building up of a track record of accuracy and precision, transparent methodology and review processes (Davis et al., 2017, p. 17).

Also, the creation of an independent institution for the attribution of cyber attacks modeled

after the International Atomic Energy Agency (IAEA) has been discussed (Smith, 2017; Healey et al., 2014). This could be an important addition to a transparent public debate about each attack within the affected nation, especially concerning attacks on less liberal societies, which are not fit to provide the necessary conditions for internal transparent debates.

At this moment of history, which is characterised by the declining relevance of traditional institutions of global governance, it does actually not seem to be the case that "the UN Security Council has the necessary resources and the political and coercive power" to attribute and to sanction cyber attacks, such as argued by Taddeo (Taddeo, 2018a, p. 323). It is widely known that the UN Security Council is paralysed since the last years (Lynch, 2020; United Nations, 2019). And, even if that was not the case, an institution for the attribution of cyber attacks as independent and transparent as possible would be preferable, because these attributions are complex and nation states' incentives to abuse them for political reasons are significant.

SECTION 3: *IUS COMMUNICATIONIS:* ATTACKS ON THE PUBLIC SPHERE AS *CASUS BELLI*

In the case of cyber attacks aiming at the manipulation of elections such as exemplified by the DNC attack of 2016, it must be noted that, due to the lack of a coercive element, the first problem of credible deterrence against such attacks is that the DNC hack was probably not illegal under international law (Banks, 2017, p. 1501). The predominant "realpolitik view of the intelligence/international law relationship" is that there are few constraints to intelligence activities abroad (Deeks 2016, p. 601). And this also applies to cyber espionage (Schmitt and NATO, 2017, p. 323; Smith, 2018, p. 224).

Intelligence activities can, at best, be met with diplomatic retorsions, which are, in turn, unlikely to stop the respective behaviour.

Although, as developed in section 1, classical just war theory is primarily a means of defense against violent attacks, it also offers an adequate answer to attacks with non-violent effects, inasmuch as it focuses on the violation of rights due to an attack, rather than on its physical means or physical effects.

This also includes a focus shifted away from the criteria of coerciveness, since the violation of rights does not need to be combined with a threat in order to amount to the violation of the right to self-determination. Since to Vitoria, the right to communicate freely is the highest norm of international law (Vitoria, 1991, p. 279), also infringements of the right to communicate (*ius communicationis*) lacking explicit coerciveness can be a *casus belli*.

In Vitoria's understanding, communication has a broad range of implications that can be exemplified by the etymology of the word. Communication means communal activities between humans in general, of course speech, but also travel and trade, and, perhaps most significantly, enjoying free access to the commons, to air and sea.

All four, speech, travel, trade and access to the commons, are of great importance to his conception in terms of its political intentions, which consist in legitimising the Spanish preaching, travel and trade in the Americas in a more coherent way than his predecessors in the *duda indiana* debate, ranging from John Mair to Matías de Paz (Thumfart, 2012, pp. 76-117). To underline its importance independent from its dark pedigree: via the appropriation by Grotius,

Vitoria's *ius communicationis* gave rise to the still valid principle of the freedom of the seas (section 4).

Vitoria's stressing of communication as the highest norm goes back to his Thomist-Aristotelian communitarian heritage that was discussed in section 1. Already Aquinas wrote: "*Civitas est quaedam communicatio. Unde contra rationem civitatis esset quod cives in nullo communicarent.*" – "The State is a kind of communication, because a State, in which citizens do not communicate is impossible" (Aquinas, 1971). With his *ius communicationis,* Vitoria extends this core principle of politics from the domestic to the international realm and strengthens it, inasmuch as violating it can be a cause of war.

This becomes clear when he denies any people the right to prohibit strangers from accessing its ports, since not only the air and the sea, but also the ports were traditionally regarded as commons. And, according to him, if one is hindered from accessing the commons, this, in turn, is a legitimate reason to wage just war. Not because it presupposes violence, which hindrance usually does, but because it is a violation of one's natural right. —"If the barbarians deny the Spaniards what is theirs by the law of nations, they commit an offence (*iniuriam)* against them. Hence, if war is necessary to obtain their rights, they may lawfully go to war" (Vitoria, 1991, p. 282).

Just war is here a means of the restitution of one's natural right to access the commons and not an act of defense against a physical attack. Vitoria uses the same word *iniuria* (i.e. "injustice") as discussed in section 1, which is only obscured by the fact that the English translation uses the misleading term "harm" in the passage in section 1 and the more adequate term "offence" in the passage quoted here.

Vitoria's emphasis on communication, i.e. speech, travel, trade, accessing the commons, stems from his Aristotelian and Thomist communitarian anthropology, according to which humans can only exist in political community with others. This communitarian anthropology runs so deep at Vitoria that a human being born without citizenship is a contradiction in terms to him (Vitoria, 1991, p. 281). Equally, losing community would be equal to losing the ontological status as a human being. That is why to Vitoria, *ius communicationis* is that part of the law of nations, which is natural law and cannot be abrogated. And denying this basic access to community is a grave violation of one's natural right, which in turn can be answered with force (Thumfart, 2017, p. 207f.).

From this point of view, an attack on communication itself is rather worse than a kinetic attack and not neglectable at all. But, of course, this presupposes that one is willing to accept the broad range of implications of the term communication in Vitoria's lectures.

In spite of some remnants of the *ius communicationis* in the Law of the Sea in contemporary international law, it is of course the consensus that one is not allowed to travel everywhere and to trade freely with everyone. Why should this be different regarding an attack on a nation's public sphere that could be described as its internal communication?

One could also draw conclusions from Vitoria's *ius communicationis* that would justify a new kind of colonialism in the digital age. Analogous to understanding the individual right to access the digital commons as a human right (Thumfart, 2017, p. 207), denying a nation the right to access another nation's digital public sphere could be considered an offence. This assumption, following the intellectual history of colonialism, could be understood as the root of the digital "open door policy" that characterised the "free internet" US foreign policy approach during the

Obama administration (Thumfart, 2017, p. 214; Hanson, 2012). This approach used the demand to open up national informational spheres as a way to establish soft power, and, as it turned out, to globally collect data: a "digital imperialism" (Thumfart, 2017, p. 214; Wasik, 2015).

The contemporary post-Snowden context (De Hert and Thumfart, 2018, p. 6) is defined by a widespread re-closure of national digital spheres (Rosenberger, 2020). From this perspective, and from a perspective of international law, it makes sense to take Vitoria's *ius communicationis,* the right to communicate, from the realm of external relations, where it is largely outdated, and apply it to the realm of internal self-determination instead. International law does not require states to maintain a democratic constitution. And, although the idea of an individual human right to access the digital sphere can be considered a sensible claim, following the doctrine of self-determination, it can be assumed that every nation has the right to keep its deliberative processes within its public sphere free from intrusions of other states.

This is supported by the International Court of Justice's Nicaragua judgement (Ibid., p. 315), which the Tallinn Manual quotes as precedent for its rule 66. "A State may not intervene, including by cyber means, in the internal or external affairs of another State" (Schmitt and NATO, 2017, p. 312). In this way, the doctrine of self-determination would, for example, prohibit Russia's DNC-hacks of 2016, inasmuch as they went beyond intelligence operations and affected the US' ability to decide about its affairs.

Ohlin argues that this is only the case if it could be substantiated that Russia's hack indeed affected the outcome of the elections (Ohlin, 2017, p. 1598). One could conclude, following Ohlin, that whilst the DNC hacks themselves did not represent a *casus belli*, the injection of the obtained materials into the pre-election debate did. However, Ohlin's focus on the effects of cyber operations on the outcome of the elections does not necessarily address the adequate issue. Rather than to support a specific party, it is the aim of such attacks to undermine the credibility of national deliberative processes in general.

Concerning an application of these insights to a doctrine of just cyberwar, Smith's distinction between two kinds of non-violent cyber attacks is helpful. Whilst cyber espionage or DDoS-attacks would normally not constitute a *casus belli,* they could so if they directly targeted the agency of the other State, i.e. if they "fundamentally undermined the ability of the target State's political and social institutions to deliberate" (Smith, 2018, p. 233ff.).

The Tallinn Manual considers an even wider understanding of possible causes of war, since it discusses the issue of frequency and poses the question whether "a series of cyber incidents that individually fall below the threshold of an armed attack (…) constitute an armed attack when aggregated" (Schmitt and NATO, 2017, p. 342). So, albeit not constituting a *casus belli* by itself, permanent surveillance such as conducted by the NSA and its allied intelligence agencies, or permanent disinformation campaigns such as conducted by the Russians during the 2016 presidential elections, could constitute a just cause of war or proportionate countermeasures, especially if they create a lasting sense of mistrust in the public sphere, affecting a nation's capacity to deliberate.

In this sense, the right to self-determination includes the prohibition of "violence against the state as an informational entity", as Haataja writes in his application of Floridi's informational ethics to cyber warfare (Haataja 2019, p. 32). A similar, explicitly non-anthropocentric application of Floridi's informational ethics to just war theory has been proposed by Taddeo (Taddeo, 2014, p. 7). Such explicitly non-anthropocentric approaches are compatible with a theory of just war based on Vitoria's *ius communicationis*, which conceives of communication as

a phenomenon in its own right that can be defended by proportionate sanctions.

However, the non-anthropocentric, information-centred approach is in danger to miss the distinctively anthropocentric nature of attacks on the public sphere. Although for example disinformation campaigns and DDoS-attacks actually have non-anthropocentric features, because they are partly conducted by "artificial agents" (Taddeo, 2012, p. 113) such as bots, these non-human agents ultimately *target* the agency and judgement of really existing humans.

What must be addressed is, ultimately, the psychological dimension of a people's trust in a society's deliberative processes and the impact of lost trust on the formulation of aims, values and purposes, which are distinctively anthropocentric issues (Sleat, 2017, p. 333).

In particular, this human dimension plays a big role considering the means that states should use to internally counteract such attacks. These means should not be restricted to regulating or insulating the national informational sphere, e.g. by the prohibition of fake news and privacy laws, but need to include promoting digital and media literacy of civil society, such as, for example, included in the European Commission's respective policy recommendations (European Commission, 2018). Next to the legitimisation of proportional countermeasures against such attacks within just war ethics, the promotion of digital and media literacy of civil society should be part of a system of distributed deterrence involving the private sector and individual citizens, which will be elaborated below.

SECTION 4: PRIVATE JUST WARS. ECONOMIC ESPIONAGE, HACK BACK AND THE RIGHT TO RESIST

This section deals with the second issue that the discourse on just cyberwar usually gets wrong. Just war ethicists in the wake of Walzer derive their theories from the enlightenment model of conflicts between free and equal individuals (McMahan, 2007). This premise limits their applicability to Westphalian state-vs-state confrontations, which resemble conflicts between free and equal individuals, inasmuch as the Westphalian model largely imagines states to be as monolithic and impermeable as in-dividuals (literally: un-divideables).

However, within cyberspace, the borders of nation states became permeable; the world of cyberwars is post-Westphalian. And the typical form of cyber aggression is not a state-vs-state confrontation, but consists in economic and industrial espionage below the level of international or even political conflicts and is purely economically motivated. Given the great interest in cyberwar theory, it is indeed "rather puzzling" that the economic sphere has not been dealt with to the same extent as the political one (Magen, 2017, p. 4).

The first difficulty here is the asymmetry in these conflicts. The victims are usually private firms who keep quiet because admitting having been hacked gives companies a bad reputation (Javers, 2013). In addition to that, companies usually want to avoid direct confrontation with states, since they want to keep future business opportunities open and they do not have incentives to engage in strongman politics.

This is for example the case concerning US companies that do not speak out about Chinese hacking. China has "engaged in cyber-enabled economic espionage and trillions of dollars of intellectual property theft", claims the White House in its National Cyber Strategy from 2018 (White House, 2018). Correspondingly, Keith Alexander, the former US National Security

Agency (NSA) director, and Dennis Blair, the former director of US National Intelligence, wrote in 2017 that "Chinese companies have stolen trade secrets from virtually every sector of the American economy" (Alexander and Blair, 2017). This American claim that China currently spearheads cyber economic espionage can also be supported by examining Turkey's and the UAE's business transactions with Chinese firms (Magen, 2017, p. 14).

However, the US also has acted as a perpetrator of economic espionage, and not just as a victim. An NSA spokesperson assured that "the department does not engage in economic espionage in any domain, including cyber" (Greenwald, 2014). Nevertheless, the NSA was spying on economic targets such as the Brazilian oil giant Petrobras. Snowden also cited the German firm Siemens as one target (Kirschbaum, 2014). However, the frontlines in economic espionage are more complex than a simple transatlantic divide. The foreign intelligence agency of Germany *Bundesnachrichtendienst* (BND) has been accused of spying in collaboration with the NSA on the French firm Airbus (BBC, 2015).

In the case of economically powerful countries such as the US and Germany, the economic dependency of companies and the connected unwillingness to come out against the perpetrators play a big role. Also, economic and financial espionage can universally be legitimised with concerns regarding economic and financial security. For example, although denying the stealing of trade secrets, in 2013, the director of US National Intelligence admitted to collecting economic and financial information abroad in order to prevent economic and financial crises (Clapper, 2013).

Economic espionage surely is the elephant in the room when one talks about cyber deterrence. Whilst it constantly fosters conflicts between states that could escalate into trade wars and ultimately military conflicts, it is usually seen as a problem that concerns the private, not the public sector, an issue of criminal, not international law.

The involvement of private actors has also another aspect, inasmuch as in cyber security, public private partnerships are the rule, rather than the exception, and private entities have robust capacities to defend and to attribute attacks. "The top tech companies appear to be as powerful as States, and sometimes even more so, to prevent cyber attacks, attribute them and to respond to malicious acts" (Bannelier and Christakis, 2017, p. 10).

Especially concerning attribution, private entities have already demonstrated their skills, for example by publicly examining the attribution of the Sony hack within a group that included prominent cyber security firms such as Novetta, Kaspersky, Symantec and ThreatConnect (section 2), by verifying the attribution of the DNC hacks (section 2) or concerning the uncovering of the Russian false flag attack on the 2018 Olympic Games which involved the firms Cisco, CrowdStrike, Intezer and Kaspersky (Greenberg, 2019b).

Additionally, the legalisation of "hack-back" or "active cyber defense" is being discussed, for example in the context of the Active Cyber Defense Certainty Act proposed to US congress. Such regulations would make it legal for companies to actively attack computer networks of their attackers.

De facto, this practice has already been adopted by companies. In 2009, Google accessed foreign computers in order to gather information about a malware attack they suffered (Glosson, 2015, p. 17). In 2011, Facebook employed active defense and took control of a hacker gang's primary command-and-control server (Glosson, 2015, p. 17). During the attacks on Sony in 2014, the company allegedly fought back by launching "a counteroffensive that sought to impede the

hackers' distribution of its data" (Glosson, 2015, p. 3). The US government has not prosecuted any of these firms for having undertaken active defense measures. In the language of just war theory, the legalisation of such practices amounts to the development of a practice of private just war.

The right to wage defensive wars is one of the most significant prerogatives of sovereign states. From a Westphalian point of view, a theory of private just war is therefore highly problematic. And also concerning cyberspace, the Tallinn Manual states: "Only States may take countermeasures. For example, an information technology firm may not act on its own initiative in responding to a harmful cyber operation targeting it by styling its response as a countermeasure" (Schmitt and NATO, 2017, p. 130).

However, such a right for private actors to take countermeasures is formulated in classical just war theory, in Hugo Grotius' very first work on international law, *de jure praedae* (1604/05), where he develops the notion of a *bellum iustum privatum*, private just war. Although *de jure praedae* is not one of the works Grotius is known for, it is quite essential to his thought, since it is here where he originally develops his still valid principle of the Freedom of the Seas.

Grotius was originally commissioned by the Dutch East India Company to write a legal opinion in defense of the capture of a Portuguese ship by a ship of this company. In order to do so, Grotius appropriated the Spaniard Vitoria's arguments. This includes great irony, since the Netherlands were engaged in a war with Spain at that time and the issues of trade and colonisation, which Vitoria discussed, were precisely a great issue of conflict in that war. To make that irony perfect, Grotius employs Vitoria's argument of the *ius communicationis* that justified Iberian colonialism so that it justifies Dutch resistance against Portugal's role as a hegemon on the world seas.

If Vitoria's claim that the right to travel and trade could be defended by the force of arms was true, argues Grotius, then the Dutch could also defend their right to travel and trade freely against Portugal's and Spain's claim to a monopoly on trade on the world's seas. The fact that it was a private entity that committed this just war, which was still unthinkable to Vitoria, does not make a difference to Grotius. Such "private just war", *bellum iustum privatum*, he argues, was necessary because the confrontation took place in international waters, where there was no protection by a state available.

"Almost all of the events that gave rise to this war took place upon the ocean; but we have maintained that no one can claim special jurisdiction over the ocean with respect to locality" (Grotius, 2006, XII).

As a result, the East India Company's natural right to self-defense applies.

> Nature withholds from no human being the right to carry on private wars; and therefore, no one will maintain that the East India Company is excluded from the exercise of that privilege, since whatever is right for single individuals is likewise right for a number of individuals acting as a group (Grotius, 2006, XII).

Grotius's doctrine of private just war might seem puzzling to contemporaries, to which war, of course, can only be conducted by states. However, it has some contemporary applications. Due to the threat of piracy in international waters, for example, trade ships carry private armed

guards with them, in order to defend themselves against pirates, which also includes pre-emptive aggression, such as the firing of warning shots (Dutton, 2017).

One might argue, as the often used and abused rhetorical figure of "digital commons" suggests (e.g. Benkler, 2006), that cyberspace is, from the perspective of legal geography, comparable to an extension of the high seas through computer networks. From this perspective, one could also justify "hack-back" actions if states are demonstratively unable to guarantee the safety of private entities formally situated on their territory, but *de facto* more at home in the vastness of cyberspace.

This analogy between maritime security and cyber security has also been developed in a paper by the Carnegie Endowment (Hofmann and Levite, 2017, pp. 23-31). Such analogisation might seem like an anachronistic recourse to Grotius' age of privateers and pirates. And, of course, a doctrine of private just wars includes the danger of further weakening the already weakened rule of international law. In particular, states may become liable for the actions of non-state actors on their territory causing harm to others, which would increase international legal conflicts.

From a realistic perspective, however, to legitimise the proportionate use of cyber force by private actors in the case of attacks could significantly contribute to international stability for seven reasons.

First, the "post-territoriality" of cyberspace (De Hert and Thumfart, 2018) raises difficult legal, ethical and political dilemmas regarding states' protection of technology companies. Technology companies are usually not situated within one state's territory, but their computers, networks and stored data are usually spread out across the globe. Which country should be responsible for defending cloud-based assets? (Hofmann and Levite, 2017, p. 14) This is a difficult question. For example, problems related to national responsibilities for protecting personal data stored in the cloud arose during the Microsoft Ireland case, which led to the Cloud Act in the US (De Hert and Thumfart, 2020). Since it defies the boundaries of territories, national legislation regarding post-territorial cloud assets has a tendency to overreach. This inherently leads to jurisdictional conflicts (Thumfart and De Hert, 2018). The deterring and stabilising impact of geographical borders has to be redrawn "by redefining territory in a way that defies the original connection of the notion of territory to the land" (Hildebrandt, 2013, p. 222). Such a redefinition of territory should be more adequate to the needs of post-territorial technology companies, who, due to the lack of consequences when attacking them, represent a preferred target for cyber attacks. In cyberspace, more than ever, the borders of firms do not follow the borders of states. Therefore, a doctrine of just war focusing on the complex territoriality of private companies needs to be developed.

Second, a doctrine of just cyber war would be far too permissive if any attack on a private actor related to it would automatically lead to a just war involving nation states. Just think about a world in which every attack on Microsoft, Facebook, Apple or Amazon would automatically trigger a response by the US government, or, even worse, by the government of every territory these companies are in any way related to. A clear separation between the defensive rights of private and public entities would contribute to lowering the risk of quick escalation of cyber conflicts into kinetic conflicts involving nation states, i.e. cross-domain conflict escalation.[2]

Third (following from arguments one and two), since a complete defense of post-territorial companies by states can neither be guaranteed nor is it desirable, companies can be expected "to fill gaps in the defensive coverage that governments provide", also by active cyber defense (Hofmann and Levite, 2017, p. 14). This behaviour has been observed regarding maritime

security, where private companies are facing a similar situation and switched to active modes of self-defense. In spite of raising severe legal problems, this mode of conduct is effective in reducing piracy (Hofmann and Levite, 2017, pp. 23-31).

Fourth, the practical employment of active cyber defense has already led to the discussion of the Active Cyber Defense Certainty Act in US congress, also known as the 'hack-back bill', which would legalise such measures. Since private active self-defense in cyberspace is a reality, it is necessary to regulate it, for example along the lines of just war principles of *jus ad bellum* and *jus in bello,* such as proportionality and attribution, and *jus post bellum,* i.e. the state of affairs after the retribution. Following Vitoria's conception of *jus post bellum* (Thumfart, 2017, p. 212), one could for example make sure that active cyber defense only serves to restore the attacked party's rights and produces no financial gains or other advantages to the party undertaking measures of active cyber defense, which seems especially important considering the profit-oriented motivations of private companies. A regulation that takes the *de facto* reality into account and considers these criteria will help to deter cyber attackers and limit the scope of possible responses.

Fifth, such a limited right to exercise proportionate hack-back will contribute to stability, inasmuch as it distributes the problem of cyber defense to more actors, some of which are, in fact, better equipped to guarantee cyber security than states. States, in turn, can profit from a robust private cyber security sector, especially since public private partnerships are rather the rule than the exception in cyber security. Distributed cyber deterrence can be expected to be more effective than centralised cyber deterrence. On the other hand, if states are entirely responsible for cyber security, this represents an incentive for companies to save resources in that field, which will decrease security.

Sixth, in general, private actors follow foremost economic motivations, when attributing and defending, which are reliable in this respect and not distorted by the need for populist strongman politics that can easily lead to conflict escalation. In the field of attribution, it has already been demonstrated that private security firms can even act as a geopolitical counterweight to the states where they headquarter.[3] Kaspersky, for example, decided to regain the trust of its clients and counter the "cloud of suspicions against the Moscow-based security firm" by providing "evidence that actually bolstered the case against Russia" during the particularly complex false flag attack on the 2018 Olympics (Greenberg, 2019a, chapter 35).

Seventh, and this is crucial: if a limited right to exercise proportionate hack back is granted to private entities, there seems to be no obstacle to also granting such a right to individual citizens for the same reasons. What if states are not only incapable of protecting their citizens' rights, for instance the human right to privacy, but complicit in foreign agents' violating their citizens' rights? Although, for example the Snowden-revelations have led to an outcry all over Europe (De Hert and Thumfart, 2018, p. 6) and saved the GDPR (Rossi, 2018), national intelligence agencies have, like corporations, in fact collaborated with the NSA (Borger, 2013). If one takes the notion of distributed deterrence seriously, then all three levels of power, states, companies and individuals, need to be equipped with deterrence mechanisms that keep other actors in check.

It seems that a perpetual violation of the human right of privacy should trigger something like the "right to resist", incorporated in the German Basic Law's article 20 and reflected in the US constitution's Second Amendment, for the case that a government acts unconstitutionally. Of course, such vigilante justice is not desirable and can only be a last resort. Especially the illegal, yet non-violent means of whistleblowing in order to protect human rights where states or

companies do not comply with their duties seems an appropriate mechanism to control the abuse of state power and technological power in cyberspace.

It is strategically short sighted to conceive of such whistleblowing activities and similar resistance exclusively in terms of a subversion of states' defense capacities, such as this is the case in the US' on-going assessment of Assange, Manning and Snowden (Miller, 2020; Lee, 2020; Maloney, 2019). In the nineteen-eighties, political theorist Gene Sharp developed "civilian-based deterrence" that paradoxically relied on the anti-war movement to "make Europe unconquerable" (Thumfart, 2011; Sharp, 1983).

When it comes to cyber deterrence, nations all over the world have yet to learn that a critical and, in extreme cases, disobedient civil society poses no threat to their national cyber security, but rather can be its strongest line of defense. The same civil society forces that make life sometimes difficult for the executive branch of government, can make it even harder for a state's enemies to attack, to remain undetected and to escape retaliation.

CONCLUSION

This contribution aimed at counteracting two shortcomings of just cyberwar theory: the insufficient discussion of non-violent cyberattacks that are directed at the public sphere and the omission of the role of non-state actors. It did so by connecting contemporary research to Vitoria's and Grotius' original conceptions of international law and just war.

In section 1, I discussed the problem of the lack of immediate physical violence of cyber attacks on the public sphere. This makes it difficult to characterise them as a prohibited use of force under the UN Charter. Also, I discussed newer frameworks, such as the Tallinn Manual's effect-based and coercion-centred approach to the assessment of cyber attacks. Vitoria's conception of just war has been demonstrated to go beyond action-based, effect-based and coercion-centred approaches alike, inasmuch as it focuses on the violation of rights caused by an attack.

In *section 2*, I discussed the attribution problem in light of three well known cyber attacks: Estonia 2007, Sony 2014 and DNC 2016. Referring to Vitoria's conception of just war, the importance of a public transparent discourse on attribution has been highlighted in its crucial function for preserving the credibility of deliberative processes and building credible deterrence. I have recommended establishing an independent, international institution for attributing cyber attacks. Four theses have been developed: 1. A long lag time between attack and attribution makes deterrence difficult; 2. The more unclear the attribution, the more effective the attack; 3. The attribution problem is no preliminary problem to effective deterrence, but rather, mechanisms for solving it are part of effective deterrence; 4. The lack of explicit coerciveness makes an attack more effective.

In *section 3*, I demonstrated that Vitoria's notion of just war legitimises sanctioning attacks on the public sphere in spite of them not involving explicit coercion or physical violence. This is based on an interpretation of his *ius communicationis,* i.e. "right to communicate", that stresses the importance of deliberative processes to political self-determination. The promotion of digital and media literacy of civil society has been identified as part of a strategy of distributed deterrence involving private actors.

In *section 4*, I have demonstrated the growing importance of private actors in the context of cyber attacks. Building on Grotius' notion of *bellum iustum privatum,* i.e. "private just war", a

doctrine of active cyber defense has been formulated, when a state cannot or does not want to protect private actors' rights. This also applies to individuals such as whistleblowers. I formulated a theory of distributed cyber deterrence that equally builds on public and private actors, the latter legitimately conducting proportionate reprisals, being involved in public private partnerships and offering civilian-based deterrence. Seven lines of argument leading to this conclusion have been developed along the following ideas: 1. the post-territoriality of cloud-based assets; 2. the need for a clear separation of private conflicts from international conflicts; 3. the analogy of the success of private deterrence in the fight against piracy on the high seas; 4. legislation such as the hack-back bill; 5. stability through distributed deterrence involving various actors; 6. the economic and non-belligerent motivations of private actors; 7. the individual right to resist as a guarantee of checks and balances of digital power.

ACKNOWLEDGEMENTS

I thank the staff of *Internet Policy Review* and the editors of this special issue. In particular, I would like to thank the peer-reviewer Robert Merkel, lecturer in Software Engineering at Monash University, who contributed one paragraph on secret services to this essay. I would also like to thank the peer-reviewer Samuli Haataja, faculty member at Griffith Law School, who contributed some in-depth knowledge regarding cyber attacks and international law.

REFERENCES

Aquinas, T. (1971). *Sancti Thomae de Aquino Sententia libri Politicorum*. Corpus Thomisticum. http://www.corpusthomisticum.org/cpo.html

Arkin, W. M. (2016, December 19). What Obama Said to Putin on the Red Phone About the Election Hack. *NBC News*. https://perma.cc/5CKG-G5XC

Banks, W. (2017). State Responsibility and Attribution of Cyber Intrusions After Tallinn 2.0. *Texas Law Review*, *95*(7), 1487–1513. https://texaslawreview.org/state-responsibility-attribution-cyber-intrusions-tallinn-2-0/

Bannelier, K., & Christakis, T. (2017). *Cyber-Attacks – Prevention-Reactions: The Role of States and Private Actors*. Les Cahiers de la Revue Défense Nationale.

BBC News. (2008, January 25). Estonia fines man for 'cyber war'. *BBC News*. http://news.bbc.co.uk/2/hi/technology/7208511.stm

BBC News. (2015, May 1). Airbus to sue over US-German spying row. *BBC News*. https://www.bbc.com/news/world-europe-32542140

Benkler, Y. (2006). *The Wealth of Networks: How Social Production Transforms Markets and Freedom*. Yale University Press.

Blair, D., & Alexander, K. (2017, August 15). China's Intellectual Property Theft Must Stop. *New York Times*. https://www.nytimes.com/2017/08/15/opinion/china-us-intellectual-property-trump.html

Borger, J. (2013, November 1). GCHQ and European spy agencies worked together on mass surveillance. *The Guardian*. https://www.theguardian.com/uk-news/2013/nov/01/gchq-europe-spy-agencies-mass-surveillance-snowden

Clapper, J. R. (2013). *Statement by Director of National Intelligence James R. Clapper on Allegations of Economic Espionage*. Office of the Director of National Intelligence (ODNI. https://www.dni.gov/index.php/newsroom/press-releases/press-releases-2013/item/926-statement-by-director-of-national-intelligence-james-r-clapper-on-allegations-of-economic-espionage

Davis, J. S. I., Boudreaux, B., Welburn, J. W., Aguirre, J., Ogletree, C., McGovern, G., & Chase, M. S. (2017). *Stateless Attribution. Toward International Accountability in Cyberspace* [Report]. Rand Corporation. https://www.rand.org/pubs/research_reports/RR2081.html

De Hert, P., & Thumfart, J. (2018). *The Microsoft Ireland case and the Cyberspace Sovereignty Trilemma. Post-Territorial technologies and companies question territorial state sovereignty and regulatory state monopolies*(Working Paper No. 4/11). Brussels Privacy Hub. https://brusselsprivacyhub.eu/BPH-Working-Paper-VOL4-N11.pdf

De Hert, P., & Thumfart, J. (2020). The Microsoft Ireland case, the CLOUD Act and the cyberspace sovereignty trilemma. In *International Trends in Legal Informatics* (pp. 373–418). Editions Weblaw.

Dutton, Y. M. (2016, July 11). Fighting Maritime Piracy with Private Armed Guards [Blog post]. *Oxford Research Group*. https://www.oxfordresearchgroup.org.uk/blog/fighting-maritime-

piracy-with-private-armed-guards

European Commission. (2018). *Communication from the Commission to the European Parliament, the Council, the European Committee and the Committee of the Regions. Tackling online disinformation: A European Approach COM(2018) 236 final*. European Union. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52018DC0236&from=de

Finlay, C. (2018). Just War, Cyber War, and the Concept of Violence. *Philosophy & Technology*, *31*, 357–377. https://doi.org/10.1007/s13347-017-0299-6

Fitton, O. (2016). Cyber Operations and Gray Zones: Challenges for NATO. *Connections*, *15*(2), 109–119. https://doi.org/10.11610/Connections.15.2.08

Freedman, L. (2017). *The Future of War: A History*. Allen Lane.

Gallagher, S. (2018, January 26). Candid camera: Dutch hacked Russians hacking DNC, including security cameras. *Ars Technica*. https://arstechnica.com/information-technology/2018/01/dutch-intelligence-hacked-video-cameras-in-office-of-russians-who-hacked-dnc/

Giesen, K.-G. (2014). Justice in Cyberwar. *Ethic@ — An International Journal of Moral Philosophy*, *13*(1), 27–49. https://doi.org/10.5007/1677-2954.2014v13n1p27

Glosson, A. D. (2015). *Active Defense: An Overview of the Debate and a Way Forward* [Working Paper]. Mercatus Center at George Mason University. https://www.mercatus.org/system/files/Glosson-Active-Defense.pdf

Goldsmith, J. L. (1999). *Against Cyberanarchy* (No. 40; Occasional Papers). University of Chicago Law School. https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1001&context=occasional_papers

Greenberg, A. (2019a). *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*. Doubleday.

Greenberg, A. (2019b, October 17). The Untold Story of the 2018 Olympics Cyberattack, the Most Deceptive Hack in History. *Wired*. https://www.wired.com/story/untold-story-2018-olympics-destroyer-cyberattack/

Greenwald, G. (2014, September 5). The US's Government Secret Pans to Spy for American cooperations. *The Intercept*. https://theintercept.com/2014/09/05/us-governments-plans-use-economic-espionage-benefit-american-corporations/

Grotius, H. (2006). *Commentary on the Law of Prize and Booty* (M. J. van Ittersum, Ed.). Liberty Fund. https://oll.libertyfund.org/titles/grotius-commentary-on-the-law-of-prize-and-booty

Gstrein, O. (2020). Mapping power and jurisdiction on the internet through the lens of government-led surveillance. *Internet Policy Review*, *9*(3). https://doi.org/10.14763/2020.3.1497

Haataja, S. (2019). *Cyber Attacks and International Law on the Use of Force*. Routledge.

https://doi.org/10.4324/9781351057028

Hanson, F. (2012, March 29). Open Door Policy. *Foreign Policy*. https://foreignpolicy.com/2012/03/29/open-door-policy/

Healey, J., Mallery, J. C., Jordan, K. T., & Youd, N. V. (2014). *Confidence-Building Measures in Cyberspace: A Multistakeholder Approach for Stability and Security* [Report]. Atlantic Council. https://www.atlanticcouncil.org/in-depth-research-reports/report/confidence-building-measures-in-cyberspace-a-multistakeholder-approach-for-stability-and-security/

Hildebrandt, M. (2013). Extraterritorial jurisdiction to enforce in cyberspace?: Bodin, Schmitt, Grotius in cyberspace. *University of Toronto Law Journal*, *63*(2), 196–224. https://doi.org/10.3138/utlj.1119

Hofmann, W., & Levite, A. (2017). *Private Sector and Cyber Defense. Can Active Measures Help Stabilize Cyberspace?*[Report]. Carnegie Endowment for International Peace. https://carnegieendowment.org/2017/06/14/private-sector-cyber-defense-can-active-measures-help-stabilize-cyberspace-pub-71236

Huang, S. (2014). Proposing a Self-Help Privilege for Victims of Cyber Attacks. *The George Washington Law Review*, *82*(4), 1229–1266. http://www.gwlr.org/wp-content/uploads/2014/10/Huang_82_4.pdf

In re Warrant to Search Target Computer at Premises Unknown, 958 F. Supp. 2d 753 (S.D. Tex. 2013) (United States District Court, S.D. Texas, Houston Division 2013). https://casetext.com/case/in-re-search

Javers, E. (2013, February 25). Cyberattacks: Why Companies Keep Quiet. *CNBC*. https://www.cnbc.com/id/100491610

Jenkins, R. (2013). Is Stuxnet Physical? Does it Matter? *Journal of Military Ethics*, *12*(1), 68–79. https://doi.org/10.1080/15027570.2013.782640

Joint Statement from the Department Of Homeland Security and Office of the Director of National Intelligence on Election Security. (2016). Department of Homeland Security. https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national

Kirschbaum, E. (2014). Snowden says NSA engages in industrial espionage: TV. *Reuters*. https://www.reuters.com/article/us-security-snowden-germany/snowden-says-nsa-engages-in-industrial-espionage-tv-idUSBREA0P0DE20140126

Lee, T. B. (2020, March 13). *Chelsea Manning is out of jail after almost a year*. https://arstechnica.com/tech-policy/2020/03/chelsea-manning-is-out-of-jail-after-almost-a-year/

Lin, H. (2012). Cyber conflict and international humanitarian law. *International Review of the Red Cross*, *94*, 886,. https://doi.org/10.1017/S1816383112000811

Lucas, G. (2017). *Ethics and Cyber Warfare*. Oxford University Press. https://doi.org/10.1093/acprof:oso/9780190276522.001.0001

Lupovici, A. (2016). The “Attribution Problem” and the Social Construction of “Violence”:

Taking Cyber Deterrence Literature a Step Forward. *International Studies Perspectives*, *17*(3), 322–342. https://doi.org/10.1111/insp.12082

Lynch, C. (2020, March 27). U.N. Security Council Paralyzed as Contagion Rages. *Foreign Policy*. https://foreignpolicy.com/2020/03/27/un-security-council-unsc-coronavirus-pandemic/

Magen, S. (2017). Cybersecurity and Economic Espionage: The Case of Chinese Investments in the Middle East. *Cyber, Intelligence, and Security*, *1*(3), 3–124. https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/resources/docs/INSS-Cyber,%20Intelligence,%20and%20Security,%20Volume%201,%20No.%203.pdf

Maloney, C. (2019, March 12). The top 4 reasons Edward Snowden deserves a fair trial. *The Hill*. https://thehill.com/blogs/congress-blog/politics/487229-the-top-4-reasons-edward-snowden-deserves-a-fair-trial

Mann, M., & Daly, A. (2019). (Big) data and the north-in-south: Australia's informational imperialism and digital colonialism. *Television and New Media*, *20*(4), 379–395. https://doi.org/10.1177/1527476418806091

Matishak, M. (2018, July 18). What we know about Russia's election hacking. *Politico*. https://www.politico.com/story/2018/07/18/russia-election-hacking-trump-putin-698087

McGuinness, D. (2017, April 27). How a cyber attack transformed Estonia. *BBC News*. https://www.bbc.com/news/39655415

McKenzie, T. (2017). *Is Cyber Deterrence Possible?* Air University Press.

McMahan, J. (2007). The Sources and Status of Just War Principles. *Journal of Military Ethics*, *6*(2), 91–106. https://doi.org/10.1080/15027570701381963

McMahan, J., & McKim, R. J. (1993). The Just War and The Gulf War. *Canadian Journal of Philosophy*, *23*(4), 501–541. https://doi.org/10.1080/00455091.1993.10717333

Miller, M. (2020, June 24). Justice Department announces superseding indictment against Wikileaks' Assange. *The Hill*. https://thehill.com/policy/cybersecurity/504434-justice-department-announces-superseding-indictment-against-wikileaks

Muller, L. P., & Stevens, T. (2017). *Upholding the NATO cyber pledge: Cyber Deterrence and Resilience: Dilemmas in NATO defence and security politics* (Research Report No. 5/2017; Policy Brief). Norwegian Institute for International Affairs (NUPI). http://www.jstor.org/stable/resrep08037

Novetta. (2016). *Operation Blockbuster. Unraveling the Long Threat of the Sony Attack* [Report]. https://operationblockbuster.com/wp-content/uploads/2016/02/Operation-Blockbuster-Report.pdf

Nye, J. S. (2017). Deterrence and Dissuasion in Cyberspace. *International Security*, *41*(3), 44–71. https://doi.org/10.1162/ISEC_a_00266

Office of the Director of National Intelligence (ODNI). (2017). *Background to "Assessing*

Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution [Declassified report]. Office of the Director of National Intelligence (ODNI). https://www.dni.gov/files/documents/ICA_2017_01.pdf

Ohlin, J. D. (2017). Did Russian Cyber Interference in the 2016 Election Violate International Law? *Texas Law Review*, *95*(7), 1579–1598. https://texaslawreview.org/russian-cyber-interference-2016-election-violate-international-law/

Open Data City. (2013). *Stasi vs NSA. How much space would the filing cabinets of the Stasi and the NSA use up, if the NSA would print out their 5 Zettabytes?* Stasi versus NSA. https://opendatacity.github.io/stasi-vs-nsa/english.html

Orend, B. (2013). *The Morality of War*. Broadview Press.

Ray, C. (2011, October 24). The Weight of Memory. *New York Times*. https://www.nytimes.com/2011/10/25/science/25qna.html

Robinson, I. (2018, April 20). How Much Does the Internet Weigh? *Azo Quantum*. https://www.azoquantum.com/Article.aspx?ArticleID=68

Roscini, M. (2010). World Wide Warfare – Jus ad bellum and the Use of Cyber Force. *Max Planck Yearbook of United Nations Law*, *14*(1), 85–130. https://doi.org/10.1163/18757413-90000050

Rosenberger, L. (2020). Making Cyberspace Safe for Democracy. *Foreign Affairs*, *May/June*, 146–159.

Rossi, A. (2018). How the Snowden Revelations Saved the EU General Data Protection Regulation. *The International Spectator*, *53*, 4 95–111. https://doi.org/10.1080/03932729.2018.1532705

Schmitt, M. N., & NATO Cooperative Cyber Defence Centre of Excellence (Eds.). (2017). *Tallinn manual 2.0 on the international law applicable to cyber operations* (Second edition). Cambridge University Press.

Shachtman, N. (2009, March 11). Kremlin Kids: We Launched the Estonian Cyber War. *Wired*. https://www.wired.com/2009/03/pro-kremlin-gro/

Skopik, F., & Pahi, T. (2020). Under false flag: Using technical artifacts for cyber attack attribution. *Cybersecurity*, *3*. https://doi.org/10.1186/s42400-020-00048-4

Sleat, M. (2018). Just cyber war?: Casus belli, information ethics, and the human perspective. *Review of International Studies*, *44*(2), 324–342. https://doi.org/10.1017/S026021051700047X

Smith, B. (2017). The need for a Digital Geneva Convention [Blog post]. *Microsoft on the Issues*. https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/#sm.0001hkfw5aob5evwum620jqwsabzv

Smith, P. T. (2018). Cyberattacks as Casus Belli: A Sovereignty-Based Account. *Journal of Applied Philosophy*, *35*(2). https://doi.org/10.1111/japp.12169

Smotherman, J. W. (2016). Justified Physical Response to Cyber Attacks from Walzer's Legalist

Paradigm. *Army War College Review*, *2*(3), 43–53. https://www.jstor.org/stable/resrep11938.5

Solis, G. D. (2014). Cyber warfare. *Military Law Review*, *219*, 1–52. https://www.loc.gov/rr/frd/Military_Law/Military_Law_Review/pdf-files/219-spring-2014.pdf#page=9

State Department. (2018). *Recommendations to the President on Deterring Adversaries and Better Protecting the American People from Cyber Threats. Office of the Coordinator for Cyber Issues*.

Sullivan, L., & Schuknecht, C. (2019, April 12). As China Hacked, U.S. Businesses Turned A Blind Eye. *NPR*. https://www.npr.org/2019/04/12/711779130/as-china-hacked-u-s-businesses-turned-a-blind-eye?t=1560710524188&t=1566677585432

Taddeo, M. (2012). Information Warfare: A Philosophical Perspective. *Philosophy & Technology*, *25*, 105–120. https://doi.org/10.1007/s13347-011-0040-9

Taddeo, M. (2014). Information Warfare: The Ontological and Regulatory Gap. *Newsletter on Philosophy and Computers*, *14*(1), 13–20. https://www.researchgate.net/publication/267019306_Information_warfare_the_ontological_and_regulatory_gap

Taddeo, M. (2018a). Deterrence and norms to foster stability in cyberspace. *Philosophy & Technology*, *31*, 323–329. https://doi.org/10.1007/s13347-018-0328-0

Taddeo, M. (2018b). The Limits of Deterrence Theory in Cyberspace. *Philosophy and Technology*, *31*, 339–355. https://doi.org/10.1007/s13347-017-0290-2

The White House. (2018). *National Cyber Strategy*. https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

Thumfart, J. (2009). On Grotius's Mare Liberum and Vitoria's De Indis, Following Agamben and Schmitt. *Grotiana*, *30*, 65–87. https://doi.org/10.1163/016738309X12537002674286

Thumfart, J. (2011, March 3). Gene Sharp. Der Demokrator. *Die Zeit*. https://www.zeit.de/2011/10/Gene-Sharp

Thumfart, J. (2012). *Die Begründung der globalpolitischen Philosophie. Francisco de Vitorias Vorlesung über die Entdeckung Amerikas im ideengeschichtlichen Kontext*. Kadmos.

Thumfart, J. (2017). Francisco de Vitoria and the Nomos of the Code: The Digital Commons and Natural Law, Digital Communication as a Human Right, Just Cyber-Warfare. In *At the Origins of Modernity* (pp. 197–217). Springer. https://doi.org/10.1007/978-3-319-62998-8_11

Thumfart, J. (2013). Kolonialismus oder Kommunikation. Kants Auseinandersetzung mit Francisco de Vitorias ius communicationis. *Proceedings of the XI. International Kant Congress in Pisa*, 929–940. https://www.academia.edu/10342105/Kolonialismus_oder_Kommunikation._Kants_Auseinandersetzung_mit_Francisco_de_Vitorias_ius_communicationis

Thumfart, J., & De Hert, P. (2018, June 4). Both the US's Cloud Act and Europe's GDPR Move Far Beyond Geography, but Will Not Solve Transatlantic Jurisdictional Conflicts. *Just Security*. https://www.justsecurity.org/57346/uss-cloud-act-europes-gdpr-move-geography-solve-

transatlantic-jurisdictional-conflicts/

Tikk, E., & Kaska, K. (2010). Legal Cooperation to Investigate Cyber Incidents: Estonian Case Study and Lessons. *Proceedings of the 9th European Conference on Information Warfare and Security*, 288–294.

United Nations. (2019, January 10). *Paralysis Constricts Security Council Action in 2018, as Divisions among Permanent Membership Fuel Escalation of Global Tensions*. https://www.un.org/press/en/2019/sc13661.doc.htm

Vitoria, F. (1991). *Political Writings* (A. Pagden & J. Lawrence, Eds. & Trans.). Cambridge University Press.

Vitoria, F. (1995). *Vorlesungen I. Völkerrecht, Politik, Kirche*. (U. Horst, Ed.; Latin and German). Kohlhammer.

Vitoria, F. (1997). *Vorlesungen II. Völkerrecht, Politik, Kirche*. (U. Horst, Ed.; Latin and German). Kohlhammer.

Wasik, B. (2015, June 4). Welcome to the Age of Digital Imperialism. *New York Times Magazine*. https://www.nytimes.com/2015/06/07/magazine/welcome-to-the-age-of-digital-imperialism.html

Waxman, M. C. (2011). Cyber Attacks as 'Force' Under UN Charter Article 2(4). *International Law Studies*, *87*, 43–57. https://scholarship.law.columbia.edu/faculty_scholarship/847/

FOOTNOTES

1. Note from the editor: a previous version of this paper did not have "and companies" included. We added these two words on the wish of the author on 16 September 2020.

2. Note from the editor: a previous version of this paper did not have the words "kinetic" and "i.e. cross-domain conflict escalation" included in this sentence. We added these words on the wish of the author on 16 September 2020.

3. Note from the editor: a previous version of this paper used the expression "the private sector" instead of the more accurate "private security firms". We made the remplacement on the wish of the author on 16 September 2020.