Digital force: disrupting life, liberty and livelihood in the information age

Keulen, R.J.F. van

4 Effective Control over the Domain of Cyberspace

"*Eye for eye.*"[244]

4.1 Introduction

As explained in Chapter 3, the legitimacy of State sovereignty is dependent upon a State's *willingness* and upon its *ability* to monopolize the use of force within its sovereign spaces - especially force which is directed against the life, liberty and property of individuals under its jurisdiction or against the sovereign existence, political independence and territorial integrity of the State itself. The goal of the current chapter is to explore whether it is possible for States to monopolize the use of force in the domain of cyberspace.

The exact borders of the spaces over which a State exercises effective control are not always exactly agreed on. Philosophers and law-makers differ among themselves and among each other. The principle behind their argumentation however, is less contentious. Sovereignty requires that the State is both capable and willing to maintain effective control over these spaces.[245] Generally speaking, the spaces which fall under the sovereign domain of the State therefore follow the people of the State and they radiate out from where they live – both horizontally and vertically. Horizontally this concerns the land territory and the internal- and territorial waters radiating out from the land. Vertically this concerns both the spaces above and below the land territory, the internal waters and above and below the territorial waters. Above, this concerns the airspace above the land territory, internal waters and above the territorial waters. Below, this concerns the land below the land territory surface and the water below the water surfaces, as well as the deep-sea beds below that. Cumulatively, these spaces of land, water and air are considered to constitute the sovereign spaces of States.

Beyond these sovereign spaces exist the high seas and the fourth domain of outer space, as well as several uninhabited territories such as Antarctica. These spaces are generally considered spaces which are not the exclusive domain of States, but rather, they are for the Common Heritage of Mankind.

From the perspective of *domains of warfare*, the sovereign spaces of land, water and air line up closely with the military, navy and air forces of States. Originally, warfare was mostly

[244] The Holy Bible, King James Version, Exodus, Chapter 21, verse 24.
[245] *See supra* Section 3.4-3.5.

a single domain endeavor; people fought on land. Subsequently, as technology advanced, the domain of water was added as a domain of warfare, as supply lines over water allowed States to project their power far beyond their land territory. In the first half of the 20th century, with further technological advancement, the domain of air was added as the third domain of warfare and in the latter half of the 20th century the domain of outer space was added as the fourth domain of warfare. The domain of cyberspace is now already commonly referred to as the fifth domain of warfare,[246] but it is less clear whether it should also be considered the fourth space of State sovereignty.

A commonly exclaimed difficulty with considering the domain of cyberspace as a sovereign space is that it is unclear whether States are *able* to maintain effective control over the part of the domain of cyberspace which falls within their sovereign space, even if they would be *willing* to do so. After all, similar to the high seas, given the architecture of cyberspace, much activity in cyberspace cannot easily be monitored or controlled. Because of the anonymous nature of conduct in cyberspace, theorists on the sovereignty in cyberspace are faced with the so-called 'attribution problem'.[247] The implied reasoning behind the attribution problem is that anyone, anywhere can direct a cyber-attack of any scale against anyone, anywhere and that this can be done with complete anonymity.

Although a growing consensus is emerging among commentators that it is possible, in theory, to attribute international responsibility to States for cyber operations which are in breach of the prohibition on the threat or use-of-force pursuant to Article 2(4) of the UN Charter,[248] there has been little discussion, let alone agreement, on how to attribute this responsibility in practice. Instead, the usual approach when confronted with the practical problem of the (perceived) anonymity of operations conducted in and through cyberspace, is to eschew the attribution problem and to either admit defeat or to hope for and to await better cyber forensics in the future, while continuing to discuss the permissibility of cyber operations in theory.

If left unaddressed, this regrettable state of affairs would result in the second criterion for state legitimacy - effective control over a space – as not being met. Resultantly, State sovereignty could not be established in the domain of cyberspace. After all, as discussed in the previous chapter, the *raison d'être* of the State is the protection of the vital interests of life,

---

[246] *See* AIV/CAVV, *Cyber Warfare*, AIV (*Advisory Council on International Affairs*), No. 77 / CAVV (*Advisory Committee on Issues of Public International Law*), No. 22, December 2011, at 12; *see also War in the Fifth Domain*, The Economist, 1st July 2010, available at: http://www.economist.com/node/16478792 (accessed on 31st July 2017).
[247] *See e.g.* Schmidt, *The New Digital Age*, p. 114-120.
[248] *See infra* Section 4.4.

liberty and property for individuals and their collective vital interests of sovereign existence, political independence and territorial integrity. In the absence of being able to provide this protection, the State lacks a *raison d'être* in cyberspace (and, given the increasing move of society into cyberspace, perhaps a *raison d'être* altogether). Resultantly, without effective control over the part of cyberspace which connects to where a State's population lives, this part of cyberspace could not be considered to fall under the domain of State sovereignty.

More worryingly, given the increasing digitization of all parts of modern society – as discussed in Chapter 2 - States can benefit tremendously from disturbing, disrupting or even destroying other States through cyberspace. Additionally, as discussed in Section 3.2, pursuant to game-theory, one would expect that States will respond to such cyber operations in any way deemed necessary to (re-)establish effective deterrence. However, (re-)establishing effective deterrence is (nearly) impossible when an aggressor actor can act anonymously. Without being able to direct a counter-response at the appropriate actor, States would not be able to (re-)establish effective deterrence. Moreover, such an a-symmetrical game whereby an actor could benefit from aggressive conduct, but would not incur costs due to the absence of responsibility, would heavily favor offensive actions from all actors with the capability of conducting cyber warfare. Given such a game, this would potentially result in perpetual war in cyberspace.

Therefore, this dissertation must address the validity of the attribution problem not just in theory, but also in practice. It must be demonstrated that the attribution problem can be solved, that international responsibility can be attributed for aggressive behavior in cyberspace and that methods of response can hence be directed at the responsible aggressor so that effective deterrence can be established and sovereignty can be claimed over (parts of) the domain of cyberspace.

Thereto, international law will be used to explore whether it is possible to attribute responsibility for cyber operations which threaten people's lives, liberty and property as well as their collective representations of sovereignty, political independence and territorial integrity.

Section 4.2 will commence by setting out the international legal framework for the responsibility of States. In this section, it will be explained that in the international legal framework for the responsibility of State, there are two requirements for responsibility, namely *attributability* and *breach of an international obligation.* This section will also go into more detail on the *attributability* part of the equation.

Sections 4.3 and 4.4 will deal with the *breach of an international obligation* part of the equation.

Section 4.3 will set out the international legal framework for the use of force in general. It will become clear in this section that the most important criteria for determining whether a certain operation meets the threshold for use of force is whether its 'scale and effects' are grave enough. Note that there are many other obligations which a State may have in cyberspace – such as due diligence, neutrality or good neighborliness. These will however not be discussed here because the purposes of this dissertation is to find a minimum threshold for sovereignty in cyberspace. Obligations following from due diligence, neutrality and good neighborliness, in this sense, are luxuries.

Section 4.4 will apply this framework to the domain of cyberspace specifically. It will become clear in this section that on the one hand, international law and international lawyers have developed useful guidelines for determining whether or not specific cyber operations are in violation of the international prohibition on the use of force, but that on the other hand, that the international legal framework is still *non liquet* when it comes to specifically dealing with the question of severity of operations conducted in cyberspace. In Chapters 5 and 6, I will fill in these *lacunae* by explaining, pursuant to social contract theory as the political philosophical underpinning of State sovereignty, why cyber operations which disrupt critical infrastructures and cyber operations which engage in large-scale intellectual property theft can be regarded as uses of force.

Sections 4.5 and 4.6 will continue with taking these findings of Chapters 5 and 6 as given and make the case that, through a process of elimination, such cyber operations can be attributed to the responsible State to a sufficient degree of certainty pursuant to the international legal framework on State responsibility. Given the extensive nature of Chapters 5 and 6, it is recommended for the sake of the flow of this chapter, to read it as it is presented here and to keep in mind that the exact definitions of large-scale intellectual property theft and durable disruption of critical infrastructures will be provided later on in this dissertation.

Section 4.5 specifically will argue that there are many, high barriers which exist in order to be able to conduct cyber operations which can attain the required "scale and effects" and severity to constitute use of force pursuant to Article 2(4) UN Charter. Given this reality and as announced in Chapter 1, I will argue here that operations which can meet the threshold for use of force can be (almost exclusively) conducted under the responsibility of States. Actors other than States may engage in acts of disturbance and small-scale disruption, but, I will argue, the greater the scale and effects of a cyber operation, the more likely it is that such operations can only be conducted under the responsibility of States pursuant to the international legal framework on State responsibility. The analogy which I propose to argue this point is that the

ability to conduct such cyber operations, using highly advanced software, is comparable to the ability to conduct operations using intercontinental ballistic missiles (ICBMs), using highly advanced hardware. Although such capabilities are theoretically available to any and all, in practice these capabilities seem to be reserved to only (a couple of) States.

Section 4.6 will continue with the second part of my solution to the attribution problem. In this section I will argue that several methods can be employed, which, in practice, make it so that it is usually possible to infer the intentions behind cyber operations which constitute use of force, even when these intentions are not explicitly communicated. The analogy which I will propose here is that inferring the intention behind cyber operations bears close resemblance to terrorist operations. Even though terrorist operations are usually also conducted under a cloak of secrecy, their source and cause is often either explicitly claimed or it can be implicitly inferred in a convincing way. In this section, I also argue that false flag cyber operations are also possible in theory, but again, that this is unlikely to take place in practice, because of the specific way in which cyber operations need to be conducted. The proposed analogy I will use to argue this point is that of submarine operations. Even though submarines are arguably even more ideal for staging false flag operations, they have not been used for this purpose, despite their wide-spread availability during many times of international tensions. Although it is possible that cyber operations will at some point be used to stage false flag attacks, this is not expected to take place in a sufficient degree so as to hinder the application of international responsibility to cyber operations generally. Like so many other legal questions dealing with evidence, the attribution of international responsibility for cyber operations does not have to be perfect to be practical and to incentivize behavior of actors appropriately.

Section 4.7 will combine these different barriers to conducting cyber operations which meet the threshold for use-of-force pursuant to the international legal framework on the use-of-force, with the methods which can be employed to infer responsibility, and argue that it possible to attribute international responsibility to a sufficient degree of certainty within the international legal framework on State responsibility. I will argue that this certainty is analogous to comparable domestic- and international legal questions around certainty and evidence, such as the level of certainty pertaining to the rules around the permissibility of pre-emptive types of self-defence.

Finally, Section 4.8 will contain a summary and conclude that the attribution problem can be solved, that international responsibility can be attributed for aggressive behavior in cyberspace and that methods of response can hence be directed at the responsible aggressor so

that effective deterrence can be established and sovereignty can be claimed over (parts of) the domain of cyberspace.

4.2 The International Legal Framework for State Responsibility

Any discussion on attributability within the international legal framework starts with Article 2 of the International Law Commission's Articles on Responsibility of States for Internationally Wrongful Acts (hereinafter: "Articles on State Responsibility"), which provides that:

"There is an internationally wrongful act of a State when conduct consisting of an action or omission:

a) Is attributable to the State under international law; and
b) Constitutes a breach of an international obligation of the State."[249]

There are two necessary conditions which can be distinguished which need to be fulfilled in order to constitute an internationally wrongful act, namely 1. there needs to be *attributability* of the conduct to the State through either action or omission under international law and 2. a *breach of an international obligation* of the State which is conducting this act or omission.

In addition, Chapter V of Part One of the Articles on State Responsibility cites the circumstances which can preclude wrongfulness, such as consent, [250] self-defence, [251] countermeasures,[252] force majeure,[253] distress,[254] necessity[255] and compliance with peremptory norms.[256] These circumstances precluding wrongfulness can be regarded as the third condition for attributability for State responsibility, as none of these six circumstances may be present in order for responsibility for a breach of an international obligation to be attributed.

This chapter contains further discussion on the former two elements of State responsibility, as the circumstances precluding wrongfulness are not in contention here.[257] If

[249] *See* International Law Commission, Responsibility of States for Internationally Wrongful Acts, G.A. Res. 56/83 annex, U.N. Doc. A/RES/56/83 (Dec. 12, 2001) (hereinafter: Articles on State Responsibility), art. 2.
[250] Art. 20 Articles on State Responsibility.
[251] Art. 21 Articles on State Responsibility.
[252] Art. 22 Articles on State Responsibility.
[253] Art. 23 Articles on State Responsibility.
[254] Art. 24 Articles on State Responsibility.
[255] Art. 25 Articles on State Responsibility.
[256] Art. 26 Articles on State Responsibility.
[257] *See* Tallinn Manual 2.0 on the International Law applicable to Cyber Operations (2017) (hereinafter: Tallinn Manual 2.0), R. 19: "The wrongfulness of an act involving cyber operations is precluded in the case of: (a) consent; (b) self-defence; (c) countermeasures; (d) necessity; (e) *force majeure*; or (f) distress."; *see also* Tallinn Manual 2.0, R. 19, cmt. 1: "This Rule is based on the grounds set forth in Part One, Chapter V, of the Articles on State

there exists a circumstance which precludes wrongfulness in physical space, then it will apply to a situation in cyberspace as well and *vice versa*.[258] There is little reason to expect that these circumstances will have different interpretations in the domain of cyberspace which would warrant discussion here.[259] Insofar as the application of the rules on the circumstances precluding wrongfulness will have different interpretations, this is beyond the topic of study of this dissertation. This dissertation deals with the political philosophical underpinnings of State sovereignty as it applies to cyberspace. It is to be expected that other studies will deal with circumstances precluding wrongfulness in cyberspace in more depth and detail, but for the purposes of this dissertation, these exact nuances are not required here. As such, this chapter will not contain further discussion of the circumstances precluding wrongfulness.

When international responsibility can be 1. attributed to a State for an act or omission 2. which constitutes a breach of an international obligation and 3. when there are no circumstances precluding wrongfulness, then there are several consequences for the State in question. The State in question is required to continue to perform the duty of the obligation which has been breached,[260] to cease the breach of the obligation and to provide appropriate assurances of this[261] and to provide reparations,[262] regardless of whether a State's internal legal system is in conflict with the international obligations which have been breached.[263]

Moreover, this responsibility can be attributed to a State through a variety of ways. Chapter II of Part One of the Articles on State Responsibility deals with the attribution of conduct to a State. States have a wide and growing variety of responsibilities and not just for conduct of organs of the State itself.[264] In addition to this traditional type of responsibility, a State also bears responsibility for conduct by persons or entities exercising elements of governmental authority,[265] for conduct by organs placed at the disposal of a State by another State,[266] for excess of authority or contravention of instructions by an organ of a State or by a

Responsibility. Should one of the enumerated circumstances exist, the action or omission in question will not be 'wrongful' and, therefore, the State engaging in the, or omitting required, conduct will not bear responsibility for what would otherwise be a wrongful breach of an obligation owed to the injured State"; *see also generally* R. 20-31.

[258] *See generally* Tallinn Manual 2.0, R. 19; *see also generally* R. 20-31.
[259] *See* generally Tallinn Manual 2.0, R. 19; *see also generally* R. 20-31.
[260] Art. 29 Articles on State Responsibility.
[261] Art. 30 Articles on State Responsibility.
[262] Artt. 31, 34-39 Articles on State Responsibility.
[263] Art. 32 Articles on State Responsibility.
[264] Art. 4 Articles on State Responsibility.
[265] Art. 5 Articles on State Responsibility.
[266] Art. 6 Articles on State Responsibility.

person or entity empowered to exercise certain elements of the governmental authority,[267] for conduct directed or controlled by a State,[268] for conduct carried out in the absence or default of the official authorities,[269] for conduct of an insurrectional or other movement which becomes the new government[270] and for conduct acknowledged and adopted by a State as its own.[271]

In these abovementioned responsibilities, we can discern a scale of control which the State has over the conduct. The State has much more control over the conduct by organs of the State itself than it has over conduct which has been carried out by actors who are not directly part of State organs and over acts or omissions which are merely acknowledged and adopted by a State *post-facto*. In the case of conduct of organs of the State itself, the State can directly decide who to hire, fire, promote or demote, based on criteria it sets. Even in the case of actions or omissions which have been conducted in excess of authority or in contraventions of instructions, the State can do so and can hence have much control over conduct. In the case of the later categories mentioned in the previous paragraph – such as conduct by persons or entities exercising, conduct by organs placed at the disposal of a State by another State, conduct directed or controlled by a State, conduct carried out in the absence or default of the official authorities, conduct of an insurrectional or other movement which becomes the new government or conduct acknowledged and adopted by a State as its own – the control is much less direct.

Nonetheless, as mentioned, a State can be responsible for conduct both through commission and/or through omission. Furthermore, the scope of the category of omission has also expanded in recent years, in the post 9/11 world, mostly having to do with 'safe havens' for non-State actors who are engaged in acts of terrorism across State borders. Although the discussion around this expansion is still ongoing, it is generally accepted that a State can be responsible, at least in theory, for conduct not just when it is directed through its own armed forces or through proxies over which it maintains a certain level of command and control,[272] or over actions from private individuals when the State explicitly acknowledges and adopts the

[267] Art. 7 Articles on State Responsibility.
[268] Art. 8 Articles on State Responsibility.
[269] Art. 9 Articles on State Responsibility.
[270] Art. 10 Articles on State Responsibility.
[271] Art. 11 Articles on State Responsibility.
[272] *Cf*. Prosecutor v. Dusko Tadic (Appeal Judgement), IT-94-1-A, International Criminal Tribunal for the former Yugoslavia (ICTY) (hereinafter: "Tadic case"), 15 July 1999, paras. 131, 145; Case Concerning United States Diplomatic and Consular Staff in Tehran (United States of America v. Iran); Order, 12 V 81, International Court of Justice (ICJ) (hereinafter: "Tehran hostages case"), 12 May 1981; *See* Case Concerning Military and Paramilitary Activities In and Against Nicaragua (Nicaragua v. United States of America); Merits, International Court of Justice (ICJ) (hereinafter: "Nicaragua case"), 27 June 1986, para. 202.

conduct as its own,[273] but also over the conduct of private individuals when said State is willingly not interfering with their conduct and when it does have the capability to do so.[274] In other words, also implicit or tacit approval of acts committed by private individuals can create complicity and can constitute failure to comply with international obligations of good neighborliness.

According to the group of international experts (hereinafter: "Tallinn Experts") which composed the Tallinn Manual on the International Law applicable to Cyber Warfare (hereinafter: "Tallinn Manual"),[275] these general observations about the legal framework on state responsibility pursuant to the Articles on State Responsibility apply without reservation to the domain of cyberspace.[276] In Rule 6 of the Tallinn Manual, on the legal responsibility of States, the manual states that: "A State bears international legal responsibility for a cyber operation attributable to it and which constitutes a breach of an international obligation".[277] This rule, which echoes Article 2 of the Articles on State Responsibility, applies Article 2 of the Articles on State Responsibility to cyber operations and maintains that there is nothing in the nature of cyberspace or cyber operations which precludes international responsibility.[278] Hence, such responsibility can therefore be attributed under the circumstances provided in the international legal framework, as summed up in the previous paragraphs.[279] In the second edition of the Tallinn Manual on the International Law applicable to Cyber Operations (hereinafter: "Tallinn Manual 2.0), the Tallinn Experts[280] expounded upon the original Tallinn Manual when it comes to attribution of international responsibility to States for cyber operations conducted by State organs,[281] for cyber operations conducted by organs of other States[282] and for cyber operations conducted by non-State actors.[283]

---

[273] *Id.*
[274] *Id.*
[275] Tallinn Manual on the International Law Applicable to Cyber Warfare (2013) (hereinafter: "Tallinn Manual").
[276] The NATO Cooperative Cyber Defence Centre of Excellence (hereinafter: NATO CCD COE), an international military organization based in Tallinn, Estonia, and accredited in 2008 by NATO as a 'Centre of Excellence', invited an independent international group of international legal experts, which produced the Tallinn Manual.
[277] Tallinn Manual, R. 6; *see also* Tallinn Manual 2.0, R. 14: "A State bears international responsibility for a cyber-related act that is attributable to the State and that constitutes a breach of an international legal obligation.".
[278] Tallinn Manual, R. 6; Article 2 Articles on State Responsibility.
[279] *See* Tallinn Manual, R. 6; *see also generally* Tallinn Manual 2.0, R. 15-17.
[280] *Cf* Tallinn Manual, The International Group of Experts and Participants; Tallinn Manual 2.0 International Group and Other Participants, p. xii. The group of international experts which wrote and composed the Tallinn Manual 2.0 is not exactly the same as the group which wrote and composed the original Tallinn Manual.
[281] *See* Tallinn Manual 2.0, R. 15.
[282] *See* Tallinn Manual 2.0, R. 16.
[283] *See* Tallinn Manual 2.0, R. 17.

In sum, discussions on attributability within the international legal framework start with the Articles on State Responsibility. Article 2 and Chapter V of the Articles on State Responsibility describes the three basic criteria which need to be fulfilled in order for responsibility to be attributed, namely; attributability, breach of an international obligation and the absence of circumstances precluding wrongfulness. The current section has addressed the *circumstances precluding wrongfulness* and the *attributability* aspect of the equation. It has explained that a State can be responsible for both actions and omissions and that conduct can be attributed to it when it is conducted directly through its own State organs as well as less directly through a variety of other actors. This section has also explained that the international legal framework for State responsibility applies to both the physical world and to the domain of cyberspace and that it does so without reservations. The next two sections will commence with the *breach of an international obligation* part of the equation, namely a breach of the obligation of States to respect other States' sovereignty and to not engage in forceful conduct against them. Section 4.3 will deal with the international legal framework for the use of force in international relations in a general sense. Thereafter, Section 4.4 will apply this framework for the use of force in international relations to the domain of cyberspace specifically. In Chapters 5 and 6, the breach of an international obligation will be dealt with in more detail and it will be discussed how large-scale theft of intellectual property and durable disruption of critical infrastructures through cyberspace constitute use of force pursuant to the international legal framework on the use of force.

4.3 The International Legal Framework for Use of Force

The previous section has explained that there are three conditions for the attribution of State responsibility and it has addressed two of them, namely; attributability and circumstances precluding wrongfulness. The following two sections of this chapter and Chapters 5 and 6 will delve into the meat of the matter; the breaches of international obligations in the domain of cyberspace. The specific breaches of international obligations which are relevant for our discussion on maintaining effective control over a space – such as cyberspace - and for protecting life, liberty and property as well as their collective, international variants of sovereign existence, political independence and territorial integrity, revolve around the international framework on the use of force.

Any discussion on the use of force within the current international legal framework starts with Article 2(4) UN Charter, which provides that: "All Members 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".[284]

Further, in the current international legal framework on the use of force, there is a grading scale pursuant to the gravity of the force used. Although there exists a presumption of illegality for all threats or uses of force, operations which threaten the territorial integrity or political independence of a State are considered as especially egregious and as intensifiers on the use of force, since territorial integrity and political independence are the constitutive elements of the sovereign existence of the State.[285] Furthermore, if the use of force increases further in breadth, depth and duration, it can reach the threshold of an 'armed attack' pursuant to Article 39 UN Charter.[286] Furthermore, below the threshold for use of force pursuant to Article 2(4) UN Charter, we find non-forceful types of coercion – such as economic and political coercion.[287] Corresponding to the method and measure of coercion applied against a State's right to self-determination, there exists a continuum of gravity along which we find non-forceful coercion, use of force, use of force against political independence and territorial integrity and armed attack exist, respectively. Not all coercion is created equally.

Correspondingly, depending on the threshold which is reached – whether it is coercion, use of force, use of force against political independence and territorial integrity or armed attack – the response to these measures of coercion needs to correspond to the appropriate threshold. For example, when a method of coercion reaches the threshold for armed attack, legal self-defence is allowed pursuant to Article 51 UN Charter,[288] whereas use of force pursuant to 2(4) UN Charter will only lawfully permit certain non-military counter-measures in response, which do not include the use of force.[289] In other words, the response from a State whose right to self-determination has been breached by another State must be proportional to the breach of this

[284] Article 2(4) UN Charter.
[285] *See supra* Section 3.5; *see also* Ruys, 'Armed Attack' and Article 51 of the UN Charter Evolutions in Customary Law and Practice, p. 152-157
[286] Article 39 UN Charter; *see also* Tallinn Manual, R. 11, cmt. 6-7.
[287] *See* Tallinn Manual, R. 11, cmt. 2.
[288] Article 51 UN Charter: "Nothing in the present Charter shall impair the inherent right of individual or collective self-defence *if an armed attack occurs against a Member of the United Nations*, until the Security Council has taken measures necessary to maintain international peace and security. ". (emphasis added)
[289] Art. 22 Articles on State Responsibility.

latter State of the *tranquilitas ordinis* as was covered extensively in Sections 3.4-3.5.[290] Order must be restored through a level of coercion which corresponds to the transgression to the *tranquilitas ordinis,* possibly supplemented only with an additional element of force necessary to create effective deterrence.[291] When States respond to coercion disproportionately – which is to say, to respond to coercion with more countermeasures or force than is necessary to deter the present and future wrongful actor or aggressor -, then the countermeasure or force which goes beyond the proportional response, possibly supplemented with the additional element of force necessary to create effective deterrence for potential future wrongful acts or aggression, constitutes a new act of wrongful actions or aggression. Certainly, especially in the relative chaos of international relations, not all States are always able or willing to respond proportionately. A State whose right to self-determination is inhibited through another State's coercion might not be able to properly judge the gravity of a situation or might want to exploit it for political gain.[292] Minor territorial intrusions by infantry units of one State into another State's territory can hence be responded to with small-scale artillery fire which is subsequently responded to by large-scale fire, which is subsequently responded to by aerial strikes, *et cetera*. This is how conflicts escalate, especially in the heat of the moment. These factual questions do however not change the fact that each level of coercion has responses which are proportional and responses which are disproportional and by using the appropriate response, wrongful acts and aggression can be deterred and effective control established.

Given that depending on the threshold which is reached – whether it is coercion, use of force, use of force against political independence and territorial integrity or armed attack – the response to these measures of coercion needs to correspond to the appropriate threshold, it is important to figure out which threshold is reached. According to the ICJ, this is determined by the 'scale and effects' of coercion.[293] Although the ICJ has repeatedly mentioned the

[290] *See infra* Sections 3.4-3.5.
[291] *Id.*
[292] *See supra* Section 3.5.
[293] *See* Nicaragua case, para. 195: "it may be considered to be agreed that an armed attack must be understood as including not merely action by regular armed forces across an international border, but also "the sending by or on behalf of a State of armed bands, groups, irregulars or mercenaries, which carry out acts of armed force against another State *of such gravity as to amount to" (inter alia) an actual armed attack* conducted by regular forces, "or its substantial involvement therein" […] The Court sees no reason to deny that, in customary law, the prohibition of armed attacks may apply to the sending by a State of armed bands to the territory of another State, if such an operation, *because of its scale and effects*, would have been classified as an armed attack rather than as a mere frontier incident had it been carried out by regular armed forces." (emphasis added); *see also* Oil Platforms (Islamic Republic of Iran *v*. United States of America) (hereinafter: "Oil platforms case"), Judgment of 6 November 2003, 2003 ICJ Rep. 161., para. 64: "Even taken cumulatively, and reserving, as already noted, the question of Iranian responsibility, these incidents do not seem to the Court to constitute an armed attack on the United States, of the

importance of the scale and effects of a type of coercion in order to determine whether the coercion attains the threshold for use of force, it has not specified when the 'scale and effects' of a specific type of coercion are sufficiently grave to constitute an illegal use of force or an armed attack.[294] In other words, a constitutive *de minimis* threshold for use of force or armed attack is not provided by the ICJ. Some basic assumptions can however be made. For example, the relation between 'scale' and 'effects' should be seen as a cause-and-effect-relation. In other words, 'scale' describes a specific method of coercion, whereas 'effects' describes the consequences of this case of coercion. *Scale* thus refers to the magnitude, intensity and duration of an operation, whereas *effects* refers to its consequences such as the level of destruction of a State's important elements - such as its people, economic and security infrastructure, destruction of aspects of its governmental authority (*i.e.* its political independence), or deprivation of its physical aspects (*i.e.* its territorial territory). As such, it is clear that mere frontier incidents (*e.g.*, border incidents such as minor territorial intrusions by infantry units or low-level exchange of fire across borders) will most likely not meet the *de minimis* threshold for an armed attack, even though they may contain illegal uses of force pursuant to Article 2(4) UN Charter.[295] In these cases, neither the scale, nor the effects are sufficiently grave to justify self-defence pursuant to Article 51 UN Charter. Also, it is clear that large-scale attacks (*e.g.*, artillery shelling, naval attacks, aerial strikes) most likely *will* meet the *de minimis* threshold for armed attack. Moreover, this is true even when the actually achieved effects turn out to be minimal.

As long as a method of coercion is producing (or is liable to produce) serious consequences, epitomized by territorial intrusions, human casualties or considerable destruction of property, then this coercion quickly moves up the severity continuum and may reach the threshold for use of force and possibly even for an armed attack. An increase in the severity of instruments used or the effects produced can thus move the coercion applied up the severity continuum and result in a difference in degree becoming a difference in kind. This is especially true if such a use of force is aimed at damaging a victim State's 'territorial integrity' (*i.e.* conquest of valuable territory which can be exploited by the aggressor State) or 'political independence' (*i.e.* conquest of valuable infrastructure which can be used to hold a State hostage). Such aims are regarded as intensifiers because territorial integrity and political

kind that the Court, in the case concerning *Military and Paramilitary Activities in and Against Nicaragua*, qualified as a "most grave" form of the use of force".

[294] *See* Tallinn Manual, R. 11, cmt. 2.

[295] *See* Nicaragua case, para. 195; *see also* Tallinn Manual, R. 11, cmt. 8.

independence are prejudicial to the international standing of a State as a whole.[296] By contrast, mere displays of force, such as firing a single rocket onto an uninhabited wasteland of another State, will not meet the threshold for armed attack, even when such methods of coercion easily reach the threshold for use of force and are thus in clear contravention of Article 2(4) UN Charter.

The distinction thus seems to also lie in the intended consequences behind the act, or the *animus aggressionis*. In other words, inability to execute on one's aggressive intentions does not excuse one from the appropriate proportional responses that would have been appropriate in case the aggression had been executed successfully. Also, the intention of the act needs to be aimed at producing these serious effects or consequences. If the *animus aggressionis* is not present, then counter-measures and forceful responses will not be justified, as they are unnecessary to restore the *tranquilitas ordinis*. After all, the aim of counter-measures and forceful responses is to connect negative consequences to the aggressive intentions that have led the aggressor to choose to engage in the aggressive conduct. By connecting the positive consequences which the aggressor has attained by engaging in this aggressive conduct to these negative consequences, the cost/benefit analysis changes for the aggressor, both for the past aggressive conduct which has been responded to, as well as for potential future aggressive conduct. Deterrence is established. If such aggressive intentions are not present, then such responses are hence not necessary.

The ICJ has referred to the necessity of establishing the *animus aggressionis* of conduct repeatedly – albeit implicitly. In the *Nicaragua case* the court noted concerning the sending by or on behalf of a State of forcible activities of armed bands who carry out acts of armed force against another State, that there was very little information available as to "the circumstances of these incursions or *their possible motivations*" and that this "renders it difficult to decide whether they may be treated for legal purposes as amounting, singly or collectively, to an 'armed attack'".[297] (emphasis added) In other words, in the absence of evidence which points towards the *animus aggressionis* of certain conduct, it is difficult to ascertain where this conducts needs to be placed on the severity continuum. Similarly, in the *Oil Platforms case*, the ICJ stated, concerning the Iranian mine-laying, that there was no evidence that "the mine laying

[296] *See supra* Section 3.5.
[297] *See* Nicaragua case, para. 231 "Very little information is however available to the Court as to the circumstances of these incursions or their *possible motivations*, which renders it difficult to decide whether they may be treated for legal purposes as amounting, singly or collectively, to an "armed attack" by Nicaragua on either or both States." (emphasis added)

[…] was aimed specifically at the US; and similarly it has not been established that the mine struck by the Bridgeton was laid with the specific *intention* of harming that ship, or other US vessels".[298] (emphasis added) In this case too, the ICJ demonstrates that a plausible reading of the intended consequences is consequential for the legal and moral judgment of the conduct concerned.

Although these distinctions might appear to be minor legal distinctions, they have major consequences in international relations. If there is *intent* to cause a certain level of harm to another State, then the latter State may respond with force to this conduct. Additionally, given the weak international legal order, as discussed in Section 3.5, this can include an additional element of punitive force which is necessary to create effective deterrence for potential future aggression. As discussed, such actions can escalate quickly, especially in the near anarchy of international relations where the first mentioned State now does not want to appear weak, as this would invite future aggression. If there had been no intent to cause harm to the other State, then the States could have also handled the situation without further escalation by simply settling the damages through just reparations.[299]

The difficulty with the element of intention however - which has often been identified with the concept of *mens rea* of domestic criminal law – is that it is virtually impossible to prove in the international sphere. In international relations, decisions are not made by a single person whose intentions can be easily inferred. Rather, decisions are made by complex bodies of decision-makers with single majorities, super majorities or (special) vetoes and they are also often taken behind closed doors when it comes to such security questions. The existence of the intention in international relations therefore needs to be derived from the act, or *actus reus*, itself. By the standard of the *actus reus*, some acts clearly contain the *animus aggressionis*. For example, in large-scale attacks, the *animus aggressionis* can be assumed *prima facie*, because it is inherent to the act due to the scale of the operation and due to its *prima facie* intended (potential) effects.[300] On the other hand, mere frontier incidents will *prima facie* not justify an invocation of the right to respond with large-scale force as the intention does not seem to be to effect severe consequences (although these incidents will allow for 'on-the-spot-reactions' in the field to create immediate deterrence).[301] In Chapters 5 and 6 I will discuss two types of

[298] *See* Oil Platforms case, para. 64.
[299] Artt. 31, 34-39 Articles on State Responsibility.
[300] *See* Y. Dinstein, *War, Aggression and Self-defence* (2011), p. 242-267.
[301] *Id.*

cyber operations which, judging by their *actus reus* clearly do contain the intention to effect such severe consequences, namely the large-scale theft of intellectual property and the durable disruption of critical infrastructures.

Clearly, States are most interested in the (intentions to exact certain) consequences of a specific method of coercion. After all, only actions with the deliberate purpose of exacting grave consequences are likely to result in such consequences. Accidental acts or omissions tend to have only limited, small-scale effects. Only deliberate acts with agency behind them can mobilize or unleash the necessary resources to cause grave consequences. Additionally, as we will see in Section 4.5, especially in cyberspace, only deliberate acts and omissions by *States* are likely to effect the grave consequences which would meet the use of force.

However, due to the inherent risk of subjectivity in assessments of whether or not a State's conduct has the intention to exact grave consequences (there is for example great risk of exaggeration on the receiving end of aggression by another State to create a maximum range of possible responses), the international legal framework has not taken a consequence-based approach, but rather, the international legal framework has taken an instrument-based approach to protect the *tranquilitas ordinis.*[302] The international legal framework therefore reflects an emphasis placed on the *scale* of a use of force, rather than on its *effects.*[303] The intentions (*animus aggressionis*) of States are hence derived from their actions (*actus reus*) and to which consequences these actions appear intended.[304] Consequently, pursuant to this approach and according to the general consensus of international lawyers, the instruments of economic and political coercion are presumed to fall into the category of methods of coercion which most likely will not meet the threshold for use of force, whereas military instruments are presumed to fall into the category of methods of coercion which most likely will meet the threshold for use of force.[305] However, between these two extremes there exist many gray areas - such as

[302] *See e.g.* A. Foltz, *Stuxnet, Schmitt Analysis, and the Cyber "Use-of-Force" Debate*, JFQ, 67, 2012 – 4; *see also* L. Boer, *'Echoes of Times Past'*: On the Paradoxical Nature of Article 2(4)*, Journal of Conflict & Security Law (hereinafter: "Echoes of Times Past")(2015), Vol. 20 No. 1, 5-26, at 7-13.
[303] *Id.*
[304] *See e.g.* A. Foltz, *Stuxnet, Schmitt Analysis, and the Cyber "Use-of-Force" Debate*; *see also* Tallinn Manual, R11, cmt. 2.
[305] *See* B. Simma, e.a., *The Charter of the United Nations: A Commentary* (2002), Vol. I, part I, article 2; *see also* Boer, *Echoes of Times Past*, at. 9-10: "[referring to this general consensus] Overall, controversy with regard to these categories is considered as marginal; consensus as widespread".

deliberately using the control systems of a dam to flood or parch another State.[306] Additionally, as we will see in the next section, the domain of cyberspace provides additional difficulties.

In sum, this section has commenced with the discussion of the third condition for State responsibility (besides the other two of them; attributability and circumstances precluding wrongfulness which have been discussed in the previous section), namely; the breach of an international obligation. The international obligation which this dissertation is concerned with is the cornerstone of the international legal order, namely the prohibition on the use of force pursuant to Article 2(4), as well as other thresholds on the coercion continuum. If this international obligation can be protected in cyberspace and if transgressions of this prohibition can be punished, then effective deterrence and sovereignty can be established. This section has explained that the international legal framework on the prohibition on the use of force contains different thresholds corresponding to the gravity of the method of coercion which is employed – namely coercion, use of force, use of force against political independence and territorial integrity and armed attack. In order to determine which threshold has been reached, one has to look at the scale and effects of the coercion employed, as well as at the intentions behind an operation (*animus aggressionis*), which can be derived from the actions (*actus reus*). The next section will apply this international legal framework for the use of force to the domain of cyberspace.

4.4 Applying the Use of force Framework to the Domain of Cyberspace

The previous section has set out the current international legal framework on the use of force in general. In this section, I will apply this framework to the domain of cyberspace specifically. The application of the current international legal framework on the use of force to the domain of cyberspace can, unfortunately, not simply be performed *mutatis mutandis*. The fundamentally different nature of cyberspace demands special, careful attention.

When applying the international legal framework for the use of force to the domain of cyberspace, it is important to consult the Tallinn Manual (just as was the case for the international legal framework on State responsibility, as discussed in Section 4.2). Although it does not enjoy the status of a primary source of international law pursuant to the ICJ Statute, it is likely that it (and new editions of it) will be invoked in the following years pursuant to Article

[306] *Id.*

38(1)(d) ICJ Statute as "teachings of the most highly qualified publicists of the various nations" and thus as a "subsidiary means for the determination of the rules of law".[307]

According to the manual, the international legal framework on the use of force can, in principle, be applied to the domain of cyberspace.[308] Rule 10 of the Tallinn Manual on the prohibition of threat or use of force, applies the impermissibility of the use of force in international relations to the domain of cyberspace without reservations. It does so at least in principle and in theory. Throughout the Tallinn Manual, it closely follows established international law, principles and definitions. In Rule 10 of the Tallinn Manual it echoes Article 2(4) UN Charter by stating that: "A cyber operation that constitutes a *threat or use of force against the territorial integrity* or *political independence* of any State, or that is in any other manner inconsistent with the purposes of the United Nations, is unlawful.".[309] (emphasis added) Again, we see that use of force is unlawful in international relations, including when it is conducted through or applied in the domain of cyberspace. In order to determine whether or not a specific cyber operation meets the threshold for use of force, the Tallinn Manual defines 'use of force' in Rule 11 by describing that "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*.".[310] (emphasis added) In other words, in order to apply the international legal framework on the use of force to the domain of cyberspace we similarly need to look at the scale and effects of a cyber operation. If these scale and effects are comparable to the scale and effects of a non-cyber operation, then the prohibition on the use of force applies as it would in non-cyber domains. With regards to *threats* to use force through cyberspace, Rule 12 states that making *threats* to use such force are also to be treated in the same way as would be the case when they would be applied using non-cyber instruments.[311] Similarly for self-defence, Rule 13 states that "A State that is the target of a cyber operation that *rises to the level of an armed attack* may exercise its inherent right of self-defence. *Whether a cyber operation constitutes an armed attack depends on its scale and effects*.".[312] Again, we see that the Tallinn Manual echoes

[307] Art. 38(1)(d) ICJ Statute.
[308] *See* Tallinn Manual, R. 10; *see also* Tallinn Manual 2.0, R. 68.
[309] *See* Tallinn Manual, R. 10; *see also* Tallinn Manual 2.0, R. 68.
[310] *See* Tallinn Manual, R. 11; *see also* Tallinn Manual 2.0, R. 69.
[311] *See* Tallinn Manual, R. 12; *see also* Tallinn Manual 2.0, R. 70.
[312] *See* Tallinn Manual, R. 13; *see also* Tallinn Manual 2.0, R. 71; *see also* AIV/CAVV, *Cyber Warfare*, at 21: "*Nothing in article 51 or customary international law specifically excludes a particular type of weapon or weapons system.* Conventional kinetic weapons are included of course, as are radiological weapons, poison gas, other chemical weapons, biological weapons and laser weapons. There is therefore no reason not to qualify a cyber attack against a computer or information system as an armed attack if the consequences are comparable to those of an attack with conventional or unconventional weapons. In other words, if a cyber attack leads to a significant number of fatalities or causes substantial physical damage or destruction to vital infrastructure, military platforms

established international legal practice by reflecting the continuum of coercion discussed in the previous section. Also, we see that the Tallinn Manual recognizes the possibility to invoke legal self-defence pursuant to Article 51 UN Charter when the threshold for armed attack is reached.[313] It is important to take special note of this. In principle and in theory, a State can respond to a cyber operation as if it were an armed attack by traditional kinetic means – using artillery shelling, naval attacks and aerial strikes -, provided the operation reaches the threshold for armed attack in its scale and effects. Additionally, in principle and in theory, a State can also choose to use kinetic means to respond to cyber attack. Bits can lead to being blown to bits. Finally, what this also entails, at least theoretically, is that according to one of the most forward thinking sources of international law as it pertains to the domain of cyberspace, wars can be now be started, fought and ended, all in the domain of cyberspace. Notably, this does not just entail that wars can be fought be new means, but it also entails that States who are geographically so far apart that they would previously not engage in warfare with each other due to issues of proximity, are now capable of doing so, all in cyberspace.

Similar to methods of coercion applied using non-cyber instruments, when it comes to operations conducted in cyberspace, according to the Tallinn Manual, it is thus the *scale* and *effects* of a cyber operation meets the threshold of use of force or, if more grave; armed attack. Resultantly, given that, as mentioned in Section 4.3, the ICJ has not provided a framework for determining a constitutive *de minimis* threshold for use of force or for armed attack, these same difficulties apply to cyber operations as well.

Moreover, since the possibility of cyber operations was not envisioned and discussed at the time of the drafting of the UN Charter because it did not exist back then, it is especially difficult to ascertain whether a *cyber* operation meets the threshold for use of force. After all, with the exception of *jus cogens* – such as prohibitions on genocide, piracy, slavery, torture, territorial aggrandizement and wars of aggression -, States need to consent to the rules which govern them.[314] If a State chooses not to participate in an international treaty or if they remain a persistent objector to the development of an international custom, then, with the exception of *jus cogens*, such rules generally do not apply to them. Given that cyber operations were not

---

or installations or civil property, it could certainly be qualified as an 'armed attack' within the meaning of article 51 of the UN Charter." (emphasis added).

[313] *Id.*

[314] *See e.g.* Art. 1(2) UN Charter: "To develop friendly relations among nations based on *respect for the principle of equal rights and self-determination of peoples*, and to take other appropriate measures to strengthen universal peace.". (emphasis added)

envisioned or discussed at the time of the drafting of the UN Charter, it becomes especially difficult to discuss whether and how rules are created to govern State behavior in cyberspace.

We can see these problems clearly in the scale and in the effects of cyber operations. Although the Tallinn Manual rightly observes that cyber operations which directly cause physical consequences – such as death and destruction - are considered to likely meet the threshold for the scale and effects to meet use of force pursuant to Article 2(4) UN Charter, or, if the scale and effects are larger, that they may also meet the threshold for armed attack pursuant to Article 51 UN Charter, what is less clear is what will happen when a cyber operation merely creates functional disruption. What makes this especially difficult is that, with regards to the *effects* of cyber operations, we can observe that cyber operations tend to not create *physical destruction*, but rather, mostly, *functional disruption*. Financial institutions, media outlets and power stations may be shut down, but physical destruction is usually minimal or even absent altogether. With regards to the *scale* of cyber operations, it is even more difficult to give a proper appreciation of cyber operations. After all, due to the aforementioned emphasis within the international legal system on the scale of an operation (*i.e.* the international legal system wields an instrument-based approach) one could argue that dealing with cyber operations could potentially require entirely new agreements between States relating to cyber operations specifically, as these instruments do not have the physical characteristics of traditional military instruments such as tanks, ships or airplanes.[315]

In order to apply the international legal framework on the use of force to the domain of cyberspace, it is useful here to briefly review the sources of international law. Article 38(1) ICJ Statute lists the sources of international law which can be consulted in order to ascertain whether certain conduct is permissible under international law. It reads:

> 1. The Court, whose function is to decide in accordance with international law such disputes as are submitted to it, shall apply:
>
> a. *international conventions*, whether general or particular, establishing rules expressly recognized by the contesting states;
>
> b. *international custom*, as evidence of a general practice accepted as law;

[315] *See supra* Section 4.3.

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

d. 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 determination of rules of law.

2. This provision shall not prejudice the power of the Court to decide a case ex aequo et bono, if the parties agree thereto.[316] (emphasis added)

In the traditional sense, use of force pursuant to Article 2(4) UN Charter or armed attacks pursuant to Article 51 UN Charter are operations conducted by the armed forces from one State against the territory, infrastructure or the land-, sea- or air forces of another State (and to a much lesser degree so far, from outer space). These provisions have been agreed on and they have been laid down in the UN Charter in 1945 and they can hence be used as a source of international law pursuant to Article 38(1)(a) ICJ Statute. The exact definition of what constitutes use of force or armed attack is however subject to customary international law pursuant to Article 38(1)(b) and therefore changes over time.[317] The legal definition of use of force or armed attack after the advent of cyberspace (or 'cyber territory') and the legal definition of *cyber forces* (in addition to land-, sea-, air- and space forces) hence needs to be regarded in the light of both the existing legal framework, as well as in the light of potential future developments, such as special-purpose treaties dealing with cyber sovereignty and warfare.

Clearly, it would be preferable if States would negotiate, agree on and implement international conventions and treaties in order to govern their conduct in cyberspace. Such international treaties would include special purpose, clear rules and they would enjoy the benefit of having been written with the explicit consent of the contracting party States. Such explicit consent would greatly benefit the legitimacy of the rules agreed upon. However, such a treaty seems highly unlikely in the near-future.

Given the danger of not having rules to regulate the behavior of States in cyberspace as it pertains to use of force - where there is potentially so much to gain and so much to lose through cyber operations as our lives move online - it is imperative to find workable solutions

[316] Article 38 ICJ Statute.
[317] *See* Nicaragua case, para. 176: "… it is hard to see how [the] "natural" or "inherent" right of self-defence can be other than of a customary nature, *even if its present content has been confirmed and influenced by the Charter*.". (emphasis added)

within the existing legal framework on the use of force. Michael Schmitt, the director of the Tallinn Manual project, recognized this when, back in 1999, he asserted that "any justification or condemnation of CNA [Computer Network Attacks] must be cast in terms of the use of force paradigm.".[318] In other words, even back in the 20th century, Schmitt sought to base the rules governing behavior in cyberspace not (just) on new purpose-specific international treaties, but also on the already existing international legal framework on the use of force. In addition, he thereto also sought to base these rules in their *expected future development* when it comes to cyber operations in customary international law.[319] Schmitt thus argued that determining whether a specific type of cyber coercion would attain the scale and effects to meet the use of force threshold, would entail *predicting* how States would respond to certain cyber operations in the future and how they would then use the existing international legal framework on the use of force to justify their responses.[320] In order to predict the future behavior of States and the expected development of international customary law, Schmitt proposed a list of criteria by which cyber operations and State behavior could be predicted. The criteria Schmitt proposed to use to make these predictions were later adopted and expanded upon in Rule 11, cmt. 9 of the Tallinn Manual.[321] They can arguably be regarded as a subsidiary means for the determination of rules of law – such as the interpretation of scale and effects in the international legal framework on the use of force - as the "teachings of the most highly qualified publicists of the various nations" pursuant to Article 38(1)(d) ICJ Statute.[322]

These criteria by which cyber operations and State behavior in response to them can be predicted are; severity, immediacy, directness, invasiveness, measurability of effects, military character, State involvement and presumptive legitimacy of cyber operations.[323] These Schmitt- or Tallinn criteria operate in concert and they are non-exhaustive.[324] They will be discussed in their respective order, with the exception of *severity*, which will be discussed last, as it is, in the

[318] M. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 CJTL 885 (1999), at 913 "Unless the international community is willing to adopt a *de novo* scheme for assessing the use of inter-state coercion, any justification or condemnation of CNA [Computer Network Attacks] must be cast in terms of the use of force paradigm.".
[319] Article 38(1)(b) ICJ Statute.
[320] M. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 CJTL 885 (1999), at 913 "Unless the international community is willing to adopt a *de novo* scheme for assessing the use of inter-state coercion, any justification or condemnation of CNA [Computer Network Attacks] must be cast in terms of the use of force paradigm.".
[321] *See* Tallinn Manual, R. 11, cmt. 9; *see also* Tallinn Manual 2.0, R. 69, cmt. 9.
[322] Art. 38(1)(d) ICJ Statute.
[323] *See* Tallinn Manual, R. 11, cmt. 9; *see also* Schmitt, at 914-915; *see also* Tallinn Manual 2.0, R. 69, cmt. 9.
[324] *See* Tallinn Manual, R. 11, cmt. 10; *see also* Tallinn Manual 2.0, R. 70.

words of the Tallinn Manual itself, "self-evidently" the most significant and indicative factor in the analysis.[325]

Immediacy refers to the temporal distance between the launch of a cyber operation and its effects - the more immediate the consequences, the more likely that States will regard it as use of force.[326] *Directness* is closely related to immediacy, but instead of dealing with the temporal distance between the cyber operation and its effects, it deals with the chain of causation between the cyber operation and the effects – the more clear the causal link between the cyber operation and specific effects, the more likely that States will regard it as use of force.[327] *Invasiveness* refers to the degree of intrusion of a cyber operation – the more cyber barriers have been breached in order to get there, the more likely that States will regard it as a use of force.[328] *Measurability of effects* relates closely to directness, but instead of dealing with the chain of causation of a cyber operation, measurability of effects deals with the objective assessment of the quality and quantity of the effects of a cyber operation – the more measurable the effects, the more likely that States will regard it as a use of force.[329] *Military character* refers to the connection between the cyber operation and (other) military operations taking place – the closer the connection between these types of events, the more likely that States will regard it as a use of force.[330] *State involvement* is closely related to *military character*, but instead of dealing with the connection between a cyber operation and (other) military operations, it deals with the connection between a cyber operation and a State's command and control structure – the more closely a State is involved in a cyber operation, the more likely it is that States will regard it as a use of force.[331] *Presumptive legality* refers to the ostensible nature of a cyber operation – the less closely it resembles otherwise legal behavior, the more likely that States will consider it as a use of force.[332]

The criterion of *severity* – which is the most significant and indicative of the Tallinn criteria – is unfortunately not sharply defined. The description which is provided in the Tallinn Manual and in Schmitt's article in 1999 explains that it is considered to concern the matter in which the consequences of a cyber operation impinge on critical national interests – the more

[325] *See* Tallinn Manual, R. 11, cmt. 9(a); *see also* Tallinn Manual 2.0, R. 69, cmt. 9(a).
[326] *See* Tallinn Manual, R. 11, cmt. 9; *see also* Tallinn Manual 2.0, R. 69, cmt. 9.
[327] *Id.*
[328] *Id.*
[329] *Id.*
[330] *Id.*
[331] *Id.*
[332] *Id.*

it impinges on critical national interests, the more likely that it will be considered a use of force.[333] In other words, it concerns the measure in which a specific cyber operation inhibits the full exercise of the right to self-determination of a State and its people. Hence, as demonstrated in Chapter 3, it is principally concerned with threats to the fundamental rights to life, liberty and property of individuals within a State, as well as their collective representations in a State's rights to sovereign existence, political independence and territorial integrity. As the threats to these rights increase through more coercive means, they can warrant stronger counter-measures, and, if rising to the level of 'armed attack', even warrant legal self-defence.[334]

In order to determine where a cyber operation needs to be placed along the severity continuum, the Tallinn Manual further divides the criterion of severity into the criteria of scope, intensity and duration of the consequences of a cyber operation.[335] In other words, severity needs to be understood as the breadth, depth and duration of the consequences of a cyber operation. Although these criteria seem to somewhat echo the 'magnitude, intensity and duration' mentioned in the previous section and the ICJ, it is important to note that the criteria of the Tallinn Manual refer to the *effects* of a cyber operation, whereas the abovementioned criteria from the ICJ refer to the *scale* of an operation.[336] In other words, it is the difference between cause and effect or the difference between instrument and consequence. The Tallinn Manual thus focuses on the consequences. To some extent, it could hence be argued (convincingly) that the Tallinn criteria for the international legal framework on the use of force applied to cyberspace have side-stepped the problem of the restrictive *instrument*-based approach of the international legal framework on the use of force.[337] In other words, by focusing on the *usus* and *opinio juris* of future expected State behavior, it is possible to wield the less-restrictive *consequence*-based approach for its normative framework.

[333] *See* Tallinn Manual, R. 11, cmt. 9(a); *see also* Schmitt, at 914; s*ee also* art. 22 Articles on State Responsibility; *see also* Tallinn Manual 2.0, R. 69, cmt. 9.
[334] Article 51 UN Charter; art. 21 Articles on State Responsibility.
[335] *See* Tallinn Manual, R. 11, cmt. 9(a); *see also* Schmitt, at 914. *See also* art. 22 Articles on State Responsibility; *see also* Tallinn Manual 2.0, R. 69, cmt. 9.
[336] *See supra* Section 4.3.
[337] *See also* Boer, *'Echoes of Times Past'*, at 13-16: "The effects-based approach to the use of force allows for the inclusion of major cyber attacks […] The dichotomy is false. What is more, the approach ultimately devolves into a purely effects-based one". Boer similarly concludes that Schmitt's approach has not created a synergy between the instrument- and the consequence-based approach. Rather, Schmitt seems to have sided with the 'purpose view' of Article 2(4) UN Charter contained in the "or in any other manner inconsistent with the Purposes of the United Nations" phrase of 2(4) for a reading of 2(4) as seeking to protect against the "disturbance to international peace and security" (or breach of the *tranquilitas ordinis*), regardless of the means employed thereto.

However, the Tallinn Manual thereby does not actually solve the problem of the inherent subjective nature of the consequence-based approach which was discussed in the previous section. Additionally, it creates a new problem of having to predict State behavior. Although the criteria proposed in the Tallinn Manual and the 1999 article they are based on, can provide guidance in this predictive pursuit, they do not actually provide a justification for their use. Moreover, although it provides some arguments for this, it also does not provide an actual justification as to *why* the international legal framework on the use of force can be applied to the domain of cyberspace. Given the fact that States need to consent to the rules which govern them, one has to provide convincing arguments that either the international legal framework on the use of force has become expanded with new instruments with the arrival of cyber weapons, just as it has with other weapon developments in the second half of the 20th century and that these weapons are not significantly different from cyber weapons or, alternatively, one has to provide alternative arguments that the international legal framework on the use of force can be applied to the domain of cyberspace.

It is the opinion of this present writer that the former justification, which is the basis for the Tallinn Manual as well, is not convincing. There are three main reasons for this opinion. Firstly, generally speaking, what we understand as warfare in the 21st century is conduct which is still mostly conducted on land, air and sea. Most new weapons are just modifications or extrapolations of older weapons. They are weapons which move atoms from order to disorder through kinetic means. Some cyber weapons can have similar destructive effects, but what is more often the case is that they move not atoms and materials, but bytes and information. Secondly, warfare on land, air, sea and in outer space are all types of warfare which are conducted in the three dimensions of physical space. Essentially, one side in a war defends one piece of physical space against the other side in a war which defends another piece of physical space. Even warfare in outer space – which so far is quite a marginal phenomenon - is mostly just an extension of airspace in this sense, just as the high seas are an extension of territorial waters. Cyberspace does not seem to fit easily into this understanding of what it means to engage in warfare, because its effects are not conditional upon physical proximity. Thirdly, as indicated earlier in this section, cyber warfare is generally characterized by *functional disruption* rather than by *physical destruction.* Although physical destruction would fall more neatly into the existing understanding of what it means to engage in warfare when "*its scale and effects are comparable to non-cyber operations rising to the level of a use of force.*", as

described in Rule 10 of the Tallinn Manual, the same is not true for functional disruption.[338] Given that cyber weapons are inherently geared towards taking out functionality, rather than full-on destruction, it is therefore not so easy to argue that cyber weapons are just another type of weapons whose use can be prohibited within the existing legal framework on the use of force.

Therefore, in order to be able to prohibit the use of cyber weapons, alternative arguments need to be used. I argue that it is possible to prohibit the use of cyber weapons not based on the prediction of future behavior of States and the international custom developed by future responses to them, as proposed by the Tallinn Manual, but based on, as I argued in the previous Chapter, the argument that Article 2(4) UN Charter and Article 51 UN Charter are merely attempts at codifying natural law and that natural law can hence be consulted for the interpretation of applying the concept of use of force to the domain of cyberspace.

In Chapters 5 and 6, I will dive deeper into why cyber operations which durable disrupt critical infrastructure or engage in large-scale theft of intellectual property will be regarded by States as severe enough to constitute use of force pursuant to the international legal framework on the use of force as discussed in this chapter, pursuant to social contract theory as the political philosophical underpinnings of State sovereignty, as discussed in Chapter 3 and pursuant to the factual background as discussed in Chapter 2 (*ex factis jus oritur*). The criteria which I will formulate in these chapters can hence serve as additional criteria to the Tallinn criteria to help determine the severity of cyber operations.

This chapter will continue with discussing how it is possible to attribute international legal responsibility for cyber operations which meet the threshold for use of force. Although it could be useful at this point to skip ahead to Chapters 5 and 6 so that one can get a thorough understanding of the exact threshold in severity for use of force, the remainder is written as a stand-alone piece and should not require this sharp definition for the purposes of this chapter on international attributability and effective control.

In sum, the current section has explained that operations conducted in cyberspace fall within the international legal framework on the use of force – at least in principle and in theory. In order to ascertain whether or not the scale and effects of a specific cyber operation will meet the threshold for use of force, the criteria of the Tallinn Manual can be consulted. The criterion of severity is the most significant and indicative of these criteria and it can be further divided

[338] *See* Tallinn Manual, R. 10; *see also* Tallinn Manual 2.0, R. 69.

into the scope, intensity and duration of an operation. In order to determine which consequences of cyber operation would amount to use of force or armed attack, we will hence have to predict how States will respond to certain cyber operations. We therefore have to find out which interests of a State are deemed to infringe on a State's right to self-determination. In other words, we have to look at how States would respond to the impingement of their sovereignty existence, political independence and territorial integrity. In order to further discuss the questions of severity and critical national interests, Chapters 5 and 6 I will further detail the two types of critical national interests which States will protect, namely; their critical infrastructures and the intellectual property created in their territory.

Now that we have discussed the theory of the three factors for international responsibility (attributability, breach of an international obligation and absence of circumstances precluding wrongfulness), in the remainder of the current chapter, I will discuss the practical possibility of attributing international responsibility. Thereto, I will use the case of Stuxnet to illustrate why it is possible to attribute international legal responsibility for cyber operations which meet the severity threshold for the use of force. Given this attributability, it subsequently becomes possible to wield the arsenal of permissible responses against the aggressor in order to create effective deterrence and to establish sovereignty in cyberspace.

4.5 Barriers to Entry for Attaining the Scale and Effects to Meet the Use of Force Threshold in the Domain of Cyberspace

In this section, I will counter the prevailing view of cyber operations that anyone, anywhere, can launch a cyber operation against anyone, anywhere of any magnitude and can do so with complete anonymity. If this would be the case, then States would be unable to attribute international responsibility for cyber operations and thus unable to respond to the aggressor and thus unable to create effective deterrence and claim sovereignty over cyberspace.

Even though cyber security experts in the private sector, war hawks in the public sector and popular media, looking to, respectively, sell products, attract funding or get clicks, often promulgate the view of "somebody sitting on their bed somewhere, that weighs 400 pounds"[339]

[339] Presidential candidate and Republican Nominee Donald J. Trump on the hack of the Democratic National Committee (hereinafter: "DNC") during the third Presidential Debate organized by Fox News on 19 October 2016: "I don't think anybody knows that it was Russia that broke into the DNC. She is saying 'Russia, Russia, Russia', but I don't know, maybe it was, I mean, it could be Russia, but it could also be China, *it could also be lots of other people, it also could be somebody sitting on their bed somewhere that weighs 400 pounds, okay? You don't know who broke in to DNC.* […] Now, whether that was Russia, whether that was China, whether it was another country,

has the potential to wreak havoc upon companies and countries alike, such a scenario is in fact highly unlikely because there exist many, high barriers to entry in the domain of cyber warfare which are insurmountable to nearly all non-State actors and even to most State actors. More specifically, I will argue that as the scale and effects of a cyber operation move up along the severity continuum, as discussed in Section 4.3, that there is a corresponding decreasing amount of actors who can perform such operations. Although cyberspace has an ostensibly very low barrier of entry, requiring little more than a computer and an internet connection, in fact, there are very high barriers to entry for actors who want to exercise *actual coercive effect*, and force through cyberspace, let alone launch operations whose severity would meet the threshold for an armed attack. Put simply, although it is possible for private individuals and organizations to conduct cyber operations which are inconvenient and irritating to States – such as acktivism, crime, subversion, espionage, and sabotage - cyber operations which go beyond such inconvenience and irritation seem to be the exclusive domain of (few) States.

The case of Stuxnet serves as a good example of this. It demonstrates that there are many, high barriers which need to be crossed by actors who wish to use cyber operations to attain the scale and effects to meet the use of force threshold.

Stuxnet, according to media and analyst reports, is a computer virus which is believed to have been used in the period of 2009-2012 to infect the computers in the Natanz nuclear enrichment facility in Iran in order to break its centrifuges by making them spin around- and slowing them down too fast, thereby making them spin out of control and self-destruct.[340] Stuxnet ended up physically destroying about a fifth of the facility's centrifuges and delayed Iran's development of a nuclear weapon by months or possibly even years.[341] Given that this delay provided a time-frame long enough to let the international sanctions against Iran to take

---

we don't know, because the truth is, under President Obama we've lost control of things that we used to have control over. We came in with the Internet, we came up with the Internet and I think Secretary Clinton and myself would agree very much when you look at what ISIS is doing with the Internet, they're beating us at our own game. ISIS! So we have to get very, very tough on cyber and cyber warfare. It is a huge problem. *I have a son. He's 10 years old. He has computers. He is so good with these computers, it's unbelievable. The security aspect of cyber is very very tough and maybe it's hardly doable*, but I will say: we are not doing the job we should be doing.". (emphasis added)

[340] *See e.g.* D. Sanger, *Obama Order Sped Up Wave of Cyberattacks Against Iran*, New York Times, June 1, 2012, available at: http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html (accessed on 31st July, 2017); *see also* R. Langner, *Ralph's Step-by-Step Guide to Get a Crack at Stuxnet Traffic and Behavior*, available at: https://www.langner.com/2010/09/ralphs-step-by-step-guide-to-get-a-crack-at-stuxnet-traffic-and-behavior/ (accessed on 31st July, 2017); *see also generally* D. Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power* (2012); *see also generally* K. Zetter, *Counting Down to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon* (2015)..

[341] *See e.g.* Sanger, *Obama Order Sped Up Wave of Cyberattacks Against Iran.*

effect, to come to the negotiating table and to agree to a (temporary) nuclear deal, it could be argued that this cyber weapon might have prevented Iran from developing the ultimate weapon of mass destruction; nuclear weapons. Subsequently, after a software update, the virus seemed to have escaped the facility where it eventually became discovered.[342]

Stuxnet was arguably the first cyber weapon to cause physical destruction of this magnitude and the first cyber operation which might have met the threshold for use of force pursuant to the international legal framework on the use of force. There are however three main difficulties regarding using the Stuxnet case when it comes to assessing it in the international legal framework on the use of force. Firstly, Iran has tried to downplay the impact of the virus in order to maintain an image of strength domestically and it has therefore not made a concerted effort to explain Stuxnet in terms of the international legal framework on the use of force. Given that Stuxnet affected *Iran*'s nuclear program, such a response would have furthered the development of the international legal framework on the use of force through the *usus* and *opinio juris* of customary international law. Unfortunately, this response was absent. Secondly, internationally, perhaps due to the lack of response from Iran, few States have chosen to express their views as to the legality of this cyber operation in the light of the international legal framework on the use of force. Again, such responses could have helped shape (customary) international law. Thirdly, Stuxnet did not disrupt an Iranian critical infrastructure (see Chapter 6 on critical infrastructure), but rather, a (military) research project. As such, it is argued that Stuxnet did not amount to a cyber operation which constituted a use of force against Iran, but rather that it is more likely that it was an act of (cyber) *sabotage*.[343] Although there would be a presumption of illegality for such an operation and although it would be counter to the

[342] *See e.g.* Sanger, *Obama Order Sped Up Wave of Cyberattacks Against Iran.*

[343] *Cf.* T. Rid, *Cyber War Will Not Take Place* (2013), p. 1-10, 41-45, 55-56; *see also* J. Stone, Cyber War Will Take Place (2013), Journal of Strategic Studies, 36:1, 101-108, at 105. Rid cites Clausewitz' three elements of war, namely that war is 1. violent 2. instrumental and 3. political and applies these criteria to Stuxnet. Rid concludes that Stuxnet does not meet the criteria for war because it did not have large-scale destructive consequences (violent), that Stuxnet was not clearly aimed to bend Iran's will (instrumental) and that the will of Israel to bend Iran's will was not communicated with the attack (political). Rid therefore concludes that Stuxnet qualifies merely as sabotage with small-scale destruction of things. Stone considers Rid's definition of sabotage as too expansive and claims that pursuant to Rid's definition, it could encompass much of traditional warfare activities. However, Stone arguably misreads Rid's statements slightly. Stone quotes Rid "*things are the prime targets, not humans*" and interprets it as a qualifying condition that force against things qualifies it as sabotage, rather than war. However, the full paragraph from Rid makes it clear that Rid merely used this sentence as a typification, that sabotage tends to be directed against things, rather than against people. This is not the same as saying that force against things must therefore necessarily be sabotage, but that sabotage, if it includes violence, is usually directed against things. More generally however, Stone rightly protests the prediction contained in the title of Rid's book, namely that Cyber War will not take place. Chapters 5 and 6 of this dissertation are dedicated to describing the two ways in which I expect 'cyber war' will take place.

international rules on good neighborliness, it does not necessarily meet the threshold for the use of force.

Regardless of the abovementioned lack of development of *usus* and *opinio juris*, as we will see, the case of Stuxnet does provide many valuable lessons to help explain why attributing international legal responsibility is possible for such operations. We will deal with the severity question in the upcoming two chapters. This chapter continues with the attribution question.

Reports by cyber security experts conclude that Stuxnet was an unprecedentedly complex and expertly written virus, virtually without bugs and in multiple computer programming languages (which is unusual and contributed to its unusually large size which is about 20x the size of most viruses) by presumably a team of dozens or even hundreds of extremely talented and skilled software engineers.[344] Both its so-called delivery mechanism as well as its so-called payload were unprecedented.[345] I will discuss the delivery mechanism and the payload of Stuxnet in their respective order.

First, the delivery mechanism. The delivery mechanism contained device drivers which had been digitally signed with two valid certificates. What this is means is that it allowed the virus to install itself on new computers without prompting the computer's user for permission, thereby going unnoticed.[346] These certificates were created by two well-known Taiwanese fabless manufacturing companies, namely; Realtek Semiconductor Corp. and JMicron Technology Corporation.[347] These companies and companies like it depend for their very continued existence on these certificates not being used for such purposes. Presumably therefore, these certificates were not voluntarily provided by these companies to the buildes of Stuxnet, but rather, they were stolen, probably by the intelligence services of a State. Second, the delivery mechanism of Stuxnet also exploited at least four zero-day vulnerabilities, meaning vulnerabilities in software programs which have not yet been discovered by their developers and are therefore still unpatched and open to exploitation by people and organizations who have knowledge of this exploit.[348] Each of these individual exploits – which concerned exploits in the Windows operating system - would have been extremely rare to discover due to the vast

[344] *See e.g.* R. Langner, Cracking Stuxnet, a 21st-century cyber weapon, March 2011, TED 2011, available at: http://www.ted.com/talks/ralph_langner_cracking_stuxnet_a_21st_century_cyberweapon.html (accessed on 31st July, 2017); *see also* Rid, *Cyber War Will Not Take Place*, p. 41-45.
[345] *Id.*
[346] *Id.*
[347] *Id.*
[348] *Id.*

amounts of resources Microsoft spends on making its software as secure as possible. Alternatively, these exploits would have been very expensive to buy on the black market.

Besides these elements of the delivery mechanism, the payload of Stuxnet was also extremely advanced. First, the virus was the first of its kind to contain a programmable logic controller (PLC) rootkit, which would have required inside knowledge of Siemens Supervisory Control And Data Acquisition System (SCADA) control software and knowledge of the inner workings (and failings) of uranium centrifuges.[349] In other words, the team which build Stuxnet would probably have included nuclear physicists who had intimate knowledge of or had access to the Siemens SCADA control systems.[350] It is assumed that this access was obtained through some sort of espionage or intelligence cooperation between States as the knowledges of the workings of such systems is highly restricted.[351] Second, given that the Natanz nuclear enrichment facility is not connected to the internet and updating the virus would therefore be very difficult, the development of the virus would have probably required a real-life practice run on the Iranian used IR1 type enrichment centrifuges model. Given that these centrifuges are an understandably very rare commodity, the development team would have probably have had to have had access to Libya's IR1 enrichment centrifuges when these were being shipped out of its country after it was forced to surrender its nuclear program in 2003. This again would have required the kind of intelligence access reserved for only a dozen or so States. Third, in a mission-impossible-esque style execution, the payload of Stuxnet either contained insider knowledge on how to spoof the feedback system from the centrifuges which would have otherwise activated the necessary fail safes to prevent the centrifuges from spinning into destruction or it included tools to record the way in which the centrifuges operated prior to manipulation and to subsequently send this information back to the operators of the centrifuges when the virus started manipulating the speed of the centrifuges.[352] In other words, it spoofed the operators of the centrifuges with a false data feed.

Each of these elements was an indispensable prerequisite to the success of the virus and each would have been extremely difficult for almost any actor to achieve – including for most States -, let alone achieving all of them.

[349] *Id.*
[350] *Id.*
[351] *Id.*
[352] *Id.*

From the Stuxnet case we can distill several barriers to building cyber weapons which (could) meet the use of force threshold (or beyond that). I distill the following barriers:

1. *Computer programing talent*; the designers of Stuxnet-like viruses seemed to have been the *crème-de-la-crème* of computer programmers and software architecture managers.[353] Although a new Stuxnet virus could theoretically be written by anyone with a computer and internet connection, in practice it seems that this would require immensely talented and skilled programmers. Perhaps the appropriate analogy for the likelihood of the average software developer developing cyber weapons of the quality of Stuxnet is that this is analogous to the infinite monkey theorem. This is especially true for the durable disruption of critical infrastructures and to a less extent also for the large-scale theft of intellectual property.
2. *Specific technical expertise*: In order to take out the critical infrastructure in a State, technical skills in the specific field one would like to disrupt – such as communications-, energy- and logistics infrastructures – are required.[354] In the case of large-scale intellectual property theft, the State which launches such cyber operations needs to have armies of people with knowledge of the specifically targeted industries so it knows what kind of intellectual property to look for and which domestic industry would benefit from the stolen intellectual property.[355]
3. *Software exploits*: Not only are zero day exploits and valid certificates very difficult to come by, they are also very expensive and they only become more difficult to come by and more expensive to buy the more important the software system they exploit.[356] In other words, generally speaking, the larger the coercion an actor wants to exercise with a cyber operation, the more funding is needed to purchase an appropriate amount or type of zero day exploits and valid certificates. Although it is certainly possible that an actor gains access to large vulnerabilities using a single zero day exploit, we can assume that increased vulnerability will generally be accompanied by increased security. Especially in the case of large-scale theft of intellectual property, such an actor can choose to either purchase many exploits in less widely used software, which is cheaper, or such an actor can choose to buy fewer, but more expensive exploits in more widely used software. Also, in the case

[353] *See* Rid, *Cyber War Will Not Take Place*, p. 41-45.
[354] *Id*; *see also* AIV/CAVV, *Cyber Warfare*, at 14.
[355] *Id.*
[356] *Id.*

of large-scale intellectual property theft, the cyber operation is at a greater risk of becoming discovered (because there are more victims who can notice the operation) and therefore needs to constantly buy new exploits when old ones become patched. In the case of critical infrastructure, the hardware and software is more custom designed for a particular target and therefore requires espionage and technical knowledge as well.

4. *Cost*: Employing groups of topnotch programmers who could easily sell their skills on the private markets for hundreds of thousands of dollars annually, will quickly run into the millions of dollars annually and will probably take years to complete the building of even a single weapon.[357] Also, the same is true for the aforementioned technical experts.[358] Additionally, software exploits such as zero day exploits and valid certificates can easily cost hundreds of thousands of dollars each and Stuxnet used at least four. The estimated cost for producing Stuxnet is that it ran in the tens of millions of USD and perhaps that is has even crossed the hundred million dollar mark.[359] By comparison, this is only slightly less than the cost to purchase one of the (notoriously cost-overrun) F35As, or 'Joint Strike Fighter'. Similarly for cyber operations not geared towards the disruption of critical infrastructure, cyber operations with large-scale intellectual property theft will also quickly run up the bill. Even though such operations can run with much less advanced cyber weapons, they need armies of cyber soldiers and industry experts who target companies, find the property to steal, extract it, process it for use in domestic companies and pass it on.

In addition to the quality aspect of these different types of barriers, the quantity, or height of each of these barriers has also increased with the recent development of the cyber security industry.[360] In the past decade an industry has been build which generates hundreds of billions of dollars in revenue annually for offering the best in cyber protection technology and techniques.[361] In addition to firewalls and anti-virus software, there is now software which

[357] *Id.*
[358] *Id.*
[359] *See* Langner, Cracking Stuxnet.
[360] *See* Rid, *Cyber War Will Not Take Place*, p. 9.
[361] S. Morgan, *Cybersecurity Market Reaches $75 Billion In 2015; Expected To Reach $170 Billion By 2020*, Forbes, 20th December 2015, available at: https://www.forbes.com/sites/stevemorgan/2015/12/20/cybersecurity%E2%80%8B-%E2%80%8Bmarket-reaches-75-billion-in-2015%E2%80%8B%E2%80%8B-%E2%80%8Bexpected-to-reach-170-billion-by-2020/#4adeb25730d6 (accessed on 11th February 2018).

studies user behavior to detect anomalous behavior such as copying large amounts of design ideas on external hard drives; software which engages in predictive malware detention by generating random pieces of malware and testing its success through an evolutionary process; scrambler software which gives intruders faux data to keep them occupied; education of users; multi-step verification of user identity through multiple devices, biometric data; and much more. Moreover, not only do these developments in the cyber security industry heavily benefit the defender against the attacker, but they also disproportionally benefits high-value targets - such as oil pipelines, (nuclear) power plants, communications systems, airports, military installations and other vital infrastructure - who purchase the latest and greatest in cyber protection and share best practices on how to deal with cyber threats. The more critical an infrastructure, the better protected it has become, even compared to other infrastructures. Similarly, for large companies, the increase in protection has heavily favored companies who have the most value in intellectual property to protect. Every self-respecting large company now has a Chief Information Officer (CIO), Chief Digital Information Officer (CDIO) or Chief Information Security Officer (CISO) who is as responsible for the cyber security of the company with the same level of responsibility as the Chief Financial Officer is responsible for the financial security of the company.

All of this is not to say that it has become impossible to successfully break into critical infrastructures or to successfully engage in massive intellectual property theft. Just as in the physical world, complete security is an illusion usually sold by snake oil salesmen. No matter how high the walls one erects, someone will always find a way to go over, under, around or through it. However, what it does mean, is that breaching the cyber security of critical infrastructures or companies is increasingly becoming the exclusive domain of State actors – at least when it comes to breaching the threshold for use of force pursuant to the international legal framework on the use of force.[362] Although it is certainly possible and even likely that non-State actors will manage to cross these barriers and this threshold in the future, it is also becoming increasingly likely that it will be only States who will be able to muster up the vast financial means, programming talent, and technical expertise in order to be able to do this.[363] As Rid concludes: "*This analysis leads to a conclusion that is both sobering and comforting at the same time: the attribution problem is a function of an attack's severity*".[364]

[362] *See* Rid, *Cyber War Will Not Take Place*, p. 160.
[363] *Id.*
[364] *Id.*

Given the high barriers to the development of cyber weapons, their development by non-State actors is already highly improbable and this is becoming increasingly so. Alternatively, even if non-State actors would be able to successfully build cyber weapons, these weapons would nonetheless be highly impractical for non-State actors considering the opportunity costs. For instance, the 'Avtomat Kalashnikova' or AK-47 costs between $500 and $1000 per weapon - depending on the region and market.[365] Compare this with the low-estimate of Stuxnet of $50.000.000 and a conservative estimate indicates that one cyber weapon equates to about 50.000 AK-47s, complete with ammunition. Although cyber weapons clearly have some strategic advantages because they can be smuggled on a USB-stick, as opposed to truckloads filled with rifles, it must be asserted that they are beyond the budget of most non-State actors and arguably also even beyond the budget of many State actors. A cost/benefit analysis would conclude that they are highly uneconomical. Instead, they are luxury weapons. Additionally, this luxury status is exacerbated by the relatively short shelf-life of cyber weapons.[366] Compared again to the AK-47, cyber weapons seem highly impractical in this regard as well. The AK-47 was first presented for military trials in 1946 and is still, with only minor modifications, one of the most popularly sold and used small arms, due to its ruggedness and reliability. More than six decades after its inception, the AK-47 is still an effective weapon which can be used to conduct operations which can attain the scale and effects to constitute use of force. It still kills. In contrast, cyber weapons which can attain the scale and effects to meet the threshold for use-of-force often use zero-day vulnerabilities, which, by their very terminology, expire, often within years. Although the cyber weapons can be redeployed with new zero day vulnerabilities, this would continuously require the purchase of new zero day exploits, each of which could also have fed, clothed, housed and armed a considerable number of terrorists. Moreover, given the disproportionally heavy cyber protection of high-value targets, generally speaking, attacks using conventional kinetic weapons such as AK-47s would most likely yield far superior results regardless, both in terms of financial efficiency, as well as in terms of military effectiveness. In other words, although non-State actors can engage in cyber sabotage, espionage and subversion, they realistically will not engage in the use of force in the cyber domain.

Alternatively, ostensibly, cyber weapons could be developed by States whom subsequently could pass them on to intermediary non-State actors in order to try to avoid

[365] AK-47, In: *Wikipedia*, available at: https://en.wikipedia.org/wiki/AK-47 (accessed on 31st July, 2017).
[366] *See* AIV/CAVV, *Cyber Warfare*, at 14.

responsibility for their use. Again, although this seems possible in theory, practice would suggest otherwise. The foremost reason for this is that States who support non-State actors generally tend to only support them with light, low-cost weapons. Alternatively, even if a State would pass a cyber weapon which could attain the scale and effects to constitute use of force to a non-State actor, this State can still be held responsible for the subsequent use of these weapons by these non-State actors pursuant to the international legal framework for attribution for international responsibility as set out in Section 4.2 such as articles 5-11 of the Articles on State Responsibility.[367] Additionally, practically speaking as well, cyber weapons used for the large-scale theft of intellectual property are of little use to non-State actors. Rather, they would want to use weapons with which they can durably disrupt critical infrastructures. Given that these weapons are often build for a very specific purpose – such as the disruption of a nuclear enrichment facility with a specific configuration of centrifuges, as was the case with Stuxnet – these weapons often have the seal of their creator. It will hence be very difficult to deny responsibility for the subsequent use of such purpose-build weapons. The next section will address this *modus operandi* aspect in more detail.

In sum, the proposed result of the accumulation of these barriers is that cyber operations which are capable of attaining the scale and effects to constitute 'use-of-force' pursuant to Article 2(4) UN Charter can and will only be used by (few) States and hence fall under their international legal responsibility. The analogy which I propose to understand the unlikelihood that cyber operations will be conducted by actors other than (a few) States, is that the ability to conduct such cyber operations, using highly advanced software, is comparable to the ability to conduct operations using intercontinental ballistic missiles (ICBMs), using highly advanced hardware. Coincidentally, according to Langner - who is credited with having discovered Stuxnet - even though the delivery system of Stuxnet was already complex and high-tech to an unprecedented level, the payload itself could only be described as 'rocket science'.[368] Although building such capabilities is theoretically available to any and all, in practice, building these capabilities seems to be reserved for only (a few) States. Finally, it is unlikely that these capabilities will be passed on to proxy organizations due to the fact that States who do so would continue to bear international legal responsibility for doing so.

[367] Artt. 5-11 Articles on State Responsibility.
[368] *See e.g.* Langner, Cracking Stuxnet.

4.6 Exercising Coercive Effect in the Domain of Cyberspace

Besides asking the question "who is capable?", as discussed in the previous section, Langner, in order to deduce the creator of Stuxnet, also asked the question "*Cui bono?*" ("who benefits?").[369] In addition to the barriers of cyber operations to attaining the scale and effects to meet the threshold for the use of force – as set out in the previous section – it is posited here that several methods of inference can be employed which can often make it possible to convincingly infer the intentions behind a cyber operation. This in turn would make it possible to find the actor responsible for the cyber operation, which would enable the victim State to employ the methods necessary to punish the aggression and hence to reestablish effective deterrence.

Evidently, the clearest way to infer the responsible actor behind a cyber operation is when an actor explicitly claims responsibility for an operation. Despite the inherent benefits of cyber operations as operations which can be conducted anonymously, voluntarily discontinuing this anonymity is not as unlikely as it may seem at first glance. Given the fact that cyber operations generally, inherently create disturbance and disruption rather than death and destruction, the most useful employment of a cyber weapon is often to use it as a political threat. Hence, explicit communication of the motivation (accompanied with political demands) for cyber operations is not unusual.[370]

Alternatively, even in the absence of explicitly claimed responsibility, responsibility can often be inferred convincingly by looking at the target of the cyber operation and asking the question "who benefits?". There are three main reasons why this is often possible:

1. *Targets*: As mentioned in the previous section, cyber weapons are often special-purpose build weapons, build to disrupt or disturb one particular target – especially in the case of cyber operations which target critical infrastructure. Stuxnet for example was clearly designed to target the unique configuration of the Uranium enrichment cascades at Natanz, Iran [371] It targeted frequency converters corresponding with only two companies, one of which was Iranian and build

[369] *Id.*
[370] *See* Rid, *Cyber War Will Not Take Place*, p. 140-141; *see also* Stone, Cyber War Will Take Place, at 105. Stone protests Rid's projection of historical observation on attribution into the future. Stone points out that even if it is true that in the past acts of war have always been claimed by the responsible parties, that this does not necessarily have to hold true for the future. Although this is certainly correct, it must be observed that Rid did not make an absolute statement concerning his projection, but merely that it could be indicative of a certain likelihood.
[371] *See* Langner, Cracking Stuxnet; *see also* Rid, *Cyber War Will Not Take Place*, p. 41-45, 141-143, 149-152

centrifuges.[372] In other words, this incredibly large, expensive and complicated virus was mostly build only to be used once, at one particular destination. Even though Stuxnet also spread to many computers in other companies and countries, it caused no harm on those computers because its payload was not geared towards them. Stuxnet would simply eventually delete itself from them. Given the extremely targeted nature of cyber operations which attack critical infrastructures, lists can be made of actors who benefit enough from a disturbance or disruption in a certain facility to conduct such an operation. This list can subsequently be cross-checked with a list of parties who have the capability to conduct such cyber operations pursuant to the barriers described in the previous section. Similarly for large-scale intellectual property theft, the cyber operations are built to target specific industries which compete with the industries of the State which is conducting the operation. If a cyber operation seems geared towards particular industry and specific data within that industry, then they will likely share a common source.

2. *Implicit communication*: As noted, it must be observed that most cyber operations are a use of violence and intimidation in the pursuit of political aims, *i.e.*, they are *threats* of force or forceful threats.[373] As Schmitt has rightly pointed out: "the prohibition [on the threat of use-of-force] applies only to an *explicit or implied communication of a threat*; its essence is coercive effect.".[374] In the absence of (territorial) conquest, uses of force are, in the words of Schmitt "communicative in nature". Force can only have coercive effect when it is *exercised*, so even in the absence of explicit claims of responsibility, implicit claims are often warranted to justify the great expenses of cyber operations. Since the communication of the intention is often the very purpose of the operation, targets can be very symbolic in order to communicate a specific message. For instance, in 2007 Estonia's governmental e-services were the target of a DDoS attack, almost immediately after it decided to relocate a controversial war memorial; the Bronze Soldier of Tallinn. The operations were aimed at pressuring the government to reverse this decision. (Subsequently, Estonia formed the basis for the NATO Cooperative Cyber Defence Centre of Excellence, which helped produce the Tallinn Manual.[375])

---

[372] *Id.*
[373] *See also* Rid, *Cyber War Will Not Take Place*, p. 1-3, 159-160.
[374] *See* M. Schmitt, *Cyber Operations and the Jus ad Belllum revisited*, 56 VLR 569 (2011), at 572; *see also* Tallinn Manual, R. 12, cmt. 4 "The essence of a threat is that it is explicitly or impliedly communicative in nature".
[375] *See* Rid, *Cyber War Will Not Take Place*, p. 6-9.

3. *Modus operandi*: Another way to infer the responsible party is by looking at the *modus operandi* of a cyber operation and to compare it to other operations – both those in the past and in the present and both those in physical- and in cyberspace. For instance, Stuxnet and subsequent viruses Duqu and Flame were near identical instruments in the way they were designed and worked (although their intended purpose was different).[376] Also, Stuxnet contained several references which might have been symbolical to its creators and which might have been used as a signature.[377] If responsibility has been claimed or inferred for an earlier cyber operation and a new cyber operation has the same *modus operandi* or signature, then this might lead back to its source. Additionally or alternatively, the 'accumulation of events theory' can be consulted to infer responsibility for cyber operations. In short, the accumulation of events theory (or *Nadelstichtaktik*) holds that a series of events or operations can be linked when they are connected in time, source and cause, so that they may be accumulated to either meet the thresholds for use of force or to infer the source of new operations which seem geared towards the same cause when they happened around the same time as other operations.[378] For instance, the Israeli strike on the secret Syrian nuclear reactor in the Deir ez-Zor region in 2007 was reportedly accompanied by a cyber operation which took out several air-defence systems.[379] This accumulation of events would allow the Syrian government to infer Israeli responsibility for the accompanying cyber operation as well. Besides these cyber operations to disrupt critical infrastructures, also with large-scale theft of intellectual property, the *modus operandi* can help infer responsibility. For example, when companies in one State start seeing their designs, trade secrets and others intellectual properties in the products of their competitors in other States and when it is known that the companies where this property was created had been attacked, then this would help with inferring the responsible actor.

---

[376] *See e.g.* Langner, Cracking Stuxnet.
[377] *Id.*
[378] *See also* DoD, An Assessment of International Legal Issues in Information Operations, May 1999, *available* at: http://www.fas.org/irp/eprint/io-legal.pdf (accessed on 31 July 2017), at 21-22 " State sponsorship might be persuasively established by such factors as signals or human intelligence, the location of the offending computer within a state-controlled facility, or public statements by officials. *In other circumstances, state sponsorship may be convincingly inferred from such factors as the state of relationships between the two countries, the prior involvement of the suspect state in computer network attacks, the nature of the systems attacked, the nature and sophistication of the methods and equipment used, the effects of past attacks, and the damage which seems likely from future attacks.*". (emphasis added)
[379] *See* Rid, *Cyber War Will Not Take Place*, p. 11.

The analogy which I propose with regards to inferring the intention behind cyber operations is that it bears close resemblance to inferring the intention behind terrorist operations. Even though such operations are usually also conducted under a cloak of secrecy, they are either explicitly claimed afterwards so that the responsible actors can communicate a threat of future use of force if certain conditions are not met and thus exercise force (as is usually the case) or they coincide with other operations in time, source and cause so that responsibility can still be inferred convincingly from their implicit message.

Different cyber operations will warrant different methods of inferring responsibility. For example, in the case of large-scale intellectual property theft, it is more likely that the third method of inferring responsibility will yield the best results, whereas in the case of durable disruption of critical infrastructures, it is more likely that the second method will yield the best results.

Admittedly, when asking the question "who benefits?", it must be observed that there are also indirect ways to benefit from conducting cyber operations, most notably by staging false flag operations aimed at sparking (armed) conflict between other, competing States.[380] Moreover, pursuant to game-theory such indirect benefits would arguably continue *ad infinitum*, thus ever-expanding the circle of potential benefactors. Despite the theoretical possibility of such a scenario, in practice such a scenario also seems highly improbable, or at least not more likely than false flag operations by other traditional means of military operation. The main reason for this is a corollary to the abovementioned attributes of use of force through cyber operations. As mentioned, when a cyber operation becomes larger in scale and effects, there is a corresponding increasingly large group of people involved in building the weapon and in directing the execution of the operation. Accordingly, if the operation is used to stage a false-flag attack, then the conspiracy entails a correspondingly increasingly large and diverse group of potential whistleblowers. Therefore, generally speaking, the greater the scale and effects of an operation and its subsequent fall-out, the less likely it will be that a conspiracy can be maintained. Although it is certainly theoretically possible to assemble large groups of willing conspirators (even among the generally more universalist population of computer scientists) and perhaps game others in such a way that they are unknowingly contributing towards the conspiracy as well (although the special-purpose nature of cyber weapons makes this less likely), practically speaking, it seems more likely that cyber conspiracies will fail to materialize

[380] *See* Rid, *Cyber War Will Not Take Place*, p. 159-160.

for the same reason that other conspiracies tend to fail; rational actors recognize the following simple cost/benefit analysis:

potential benefit < potential cost x chance of getting caught

After all, if a State would try to conduct a cyber operation which meets the use of force threshold and tries to stage this operation as a false flag to spark conflict between two States, then the former State risks the wrath of the latter two State and in all likelihood also that of the international community at large who might (rightly) see the international order threatened by such conduct.

The proposed result of the accumulation of these variables is that cyber operations which are capable of constituting use of force, are not likely to be used as false flag operations or at least, they are as unlikely to be used for such purposes as other operations which have the potential to attain the same scale and effects – such as bombs and bullets. A useful analogy in this regard is that of submarine operations. Even though submarines are in many ways even more ideal for staging false flag operations – since they use a small group of people who are more or less physically cut off from communicating with the outside world - they have not been used for this purpose, despite their wide-spread availability during many times of international tensions.

In sum, besides cyber forensics there are many other useful tools which can be employed by States to infer the international legal responsibility for cyber operations which can attain the scale and effects to cross the threshold for use of force. Contrary to the popular image of cyber operations being anonymous, usually, the responsible actor claims responsibility – either explicitly or implicitly.

4.7 Inferring International Legal responsibility and (Re-)Establishing Effective Deterrence in the Domain of Cyberspace

The previous two sections have made it clear that attributing international legal responsibility for cyber operations pursuant to the international legal framework on state responsibility does not just rely on the quality of the cyber forensics employed. Rather, on top of cyber forensics,

we have seen in Section 4.5 that there are many high barriers to entry for actors who want to conduct cyber operations which attain the scale and effects to meet the threshold for use of force pursuant to article 2(4) UN Charter.[381] As such, this can be expected to help narrow down the list of potential actors to (a few) States. Furthermore, as pointed out by Rid and Buchanan, the more severe the consequences of a particular cyber operation, the more likely it is that a State whose interests have been damaged will allocate additional resources to solve the attributability question.[382] Moreover, the cyber security industry continues to erect ever-higher barriers to exercising use of force through cyberspace at a pace which is faster than the development of cyber weapons. On top of cyber forensics and the higher barriers, we have seen in Section 4.6 that besides asking the question "who is capable?", we can also ask the question "who benefits?" to further narrow down the list of potential actors who are responsible for the cyber operation. We have seen that, due to the nature of cyberspace, we can expect that responsibility for cyber operations which meet the use of force threshold is usually explicitly or implicitly claimed by the responsible actor and can be convincingly inferred.

Clearly, inferring responsibility through implicit communications by and of itself would be too weak to attribute international legal responsibility for an operation. However, taken together with the barriers mentioned in Section 4.5, a cross-check between the lists of "who is capable?" and "who benefits?" will probably slim down the list of potential actors greatly, if not zero in on the responsible actor completely. Resultantly, through such a process of elimination, the responsible actor can be taken out of anonymity and be held accountable for his aggression.

Admittedly, the process of elimination by which responsibility for cyber operations which meet the use of force threshold is inferred, is not as clear or certain as is the case when the armed forces of one State invade the physical space of another State, carrying flags, badges and uniforms. Those days are however increasingly belonging to the past and they are less and less the future of warfare. There is more to gain in cyberspace than there is in physical space and this is increasingly so. (Chapters 5 and 6 will discuss this in great detail) It should be recognized that although a level of uncertainty is inherent to inferring international legal responsibility for cyber operations, such uncertainty is not new to international relations, nor is it exclusive to cyber operations. As already mentioned in the previous section, terrorism too acts anonymously, but in practice, there seem to be few problems with regards to attributing

[381] Art. 2 UN Charter.
[382] T. Rid & B. Buchanan, *Attributing Cyber Attacks*, Journal of Strategic Studies (2015), 38:1-2, 4-37, at 10.

responsibility when terrorist operations are conducted. Moreover, besides cyber- and terrorist operations, the international legal framework on the use of force also successfully deals with other types of uncertainties. Whereas cyber- and terrorist operations deal with uncertainty in the *ratione personae* of a use of force (who is the responsible actor?), we find similarly discussions in international relations and the international legal framework on the use of force when it comes of anticipatory self-defence in response to operations of which the *ratione temporis* of an operation is uncertain (when can we be convinced that a certain operation which is being prepared will be launched?). In both cases there can be no absolute certainty - nor that a specific actor is a hundred percent certain to be responsible for a cyber certain operation which has already taken place, nor that an attack which is being prepared is a hundred percent certain to be launched -, but in both cases the international legal framework provides appropriate restrictions and permissions to guide international relations pursuant to its fundamental principles of self-determination and non-interference. There is hence an appropriate balance between the restriction on State behavior and permissibility for States so that States do not feel the need to breach international obligations to act in self-preservation. Moreover, just as the permissibility of anticipatory self-defence becomes clearer as an operation comes closer to the operation being launched, so too does the attribution of international responsibility for cyber operations become clearer as the operations become more severe in scale and effects. Hence, in both cases unwarranted unilateralism can continue to be avoided and the use of force in international relations can continue to play only a minor part.

4.8 Conclusion

This chapter started with the observation that the attribution problem in cyberspace has the potential to constitute a serious challenge to State claims of sovereignty over parts of cyberspace. After all, the *raison d'être* of the State is the protection of the vital interests of life, liberty and property for individuals and their collective variants of sovereign existence, political independence and territorial integrity. In the absence of effective control over cyberspace, a State cannot claim sovereignty over this space; without deterrence in cyberspace, the State cannot provide this protection; in the absence of attribution, effective deterrence cannot be established and effective control cannot be maintained. Fortunately, this chapter has demonstrated that the attribution problem can be solved.

Section 4.2 has set out the international legal framework on State responsibility and has detailed three requirements for State responsibility; breach of an international obligation, attributability and the absence of circumstances precluding wrongfulness. The section continued with discussions on the different types of conduct which can be attributed to States and a brief discussion on the circumstances precluding wrongfulness.

Section 4.3-4.4 have set out the international legal framework on the use of force in general and commenced with applying it to the domain of cyberspace in particular, in this respective order. In Section 4.3, it became clear that there exists a continuum of gravity along which we find coercion, use of force, use of force against political independence and territorial integrity and armed attack exist, respectively. Depending on the scale and effects of a certain operation, it moves up along this continuum. When it comes to cyberspace in particular we have to ask the question what the severity of an operation is. It has been mentioned that there are two main categories of cyber operations which meet the severity criterion to attain the scale and effects to meet the threshold for use of force pursuant to the international legal framework on the use of force; disruption of critical infrastructure and large-scale theft of intellectual property. These two types of cyber operations and the question of severity question itself are discussed in further detail in the subsequent two chapters with Chapter 5 dealing with large-scale theft of intellectual property and Chapter 6 dealing with durable disruption of critical infrastructures.

Section 4.5 returned to the attributability part of the equation. The section used the case of Stuxnet to demonstrate that there are significant barriers to entry for actors who want to conduct operations in cyberspace which can meet the severity criterion to attain the scale and effects to meet the threshold for the use of force pursuant to the international legal framework on the use of force. Moreover, the section has demonstrated that the more severe a cyber operation, the more likely it is that the cyber weapon can only created under the responsibility of a State actor. Moreover, I have explained why these barriers to entry are increasing and that the list of actors who can perform such cyber operations is correspondingly decreasing. Although these barriers cannot definitively exclude the possibility that non-State actors will be able to conduct operations which will meet the threshold for the use of force, it has been explained why the likelihood of such an occurrence is incredibly low and that it is becoming increasingly less likely.

In Section 4.6, I added another tool for attributing international legal responsibility for cyber operations which meet the use of force threshold pursuant to the international legal

framework on the use of force. I have demonstrated that even with cyber operations, it is usually possible to infer responsibility because such operations, because of their nature, are usually explicitly or implicitly claimed.

In Section 4.7, I have put the different tools for attributing international responsibility together and argued that, cumulatively, they can be wielded as a process of elimination for inferring responsibility. I discussed why this will provide a level of certainty which is sufficient to maintain international order and effective deterrence between States.

In sum, this chapter has explained why it is possible to attribute responsibility within the international legal framework on State responsibility for cyber operations whose scale and effects meet the threshold for use of force under article 2(4) UN Charter.[383] Given that it is possible to solve the attribution problem, it is therefore possible to respond to aggressions through cyberspace appropriately and hence, that it is possible to establish the effective deterrence and maintain the effective control over the domain of cyberspace which are a necessary requirement for exercising sovereignty over a domain.

Even in cyberspace, if a man contemplates striking another man's eye, then this man can expect the latter man to respond in kind so as to (re)establish effective deterrence.

[383] Art. 2(4) UN Charter.

PORTIA

Tarry, Jew

The law hath yet another hold on you.

It is enacted in the laws of Venice,

If it be proved against an alien

That by direct or indirect attempts

He seek the life of any citizen,

The party 'gainst the which he doth contrive

Shall seize one half his goods. The other half

Comes to the privy coffer of the state,

And the offender's life lies in the mercy

Of the Duke only 'gainst all other voice.

In which predicament I say thou stand'st,

For it appears by manifest proceeding

That indirectly—and directly too—

Thou hast contrived against the very life

Of the defendant, and thou hast incurred

The danger formerly by me rehearsed.

Down, therefore, and beg mercy of the Duke.

GRATIANO

Beg that thou mayst have leave to hang thyself,

And yet, thy wealth being forfeit to the state,

Thou hast not left the value of a cord.

Therefore thou must be hanged at the state's charge.

DUKE

That thou shalt see the difference of our spirit,

I pardon thee thy life before thou ask it.

For half thy wealth, it is Antonio's.

The other half comes to the general state,

Which humbleness may drive unto a fine.

PORTIA

Ay, for the state, not for Antonio.

SHYLOCK

Nay, take my life and all. Pardon not that.

You take my house when you do take the prop

That doth sustain my house. You take my life

When you do take the means whereby I live.[384]

[384] W. Shakespeare, The Merchant of Venice (Original text), *available at*: http://nfs.sparknotes.com/merchant, Act 4, Scene 1, Page 15-16, lines 338-369.