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

Keulen, R.J.F. van

Universiteit Leiden

Digital Force: Disrupting Life, Liberty and Livelihood in the Information Age

Roy van Keulen

Blanco Pagina / Blanc page

DIGITAL FORCE: DISRUPTING LIFE, LIBERTY AND LIVELIHOOD IN THE INFORMATION AGE

PROEFSCHRIFT

ter verkrijging van

de graad van Doctor aan de Universiteit Leiden,

op gezag van Rector Magnificus prof. mr. C.J.J.M. Stolker,

volgens besluit van het College voor Promoties

te verdedigen op woensdag 9 mei 2018

klokke 16.15 uur

door

Roy Johan Frank van Keulen

geboren te Beverwijk

in 1986

Promotor:	Prof. dr. A. Ellian
Co-promotor:	Dr. G. Molier

Promotiecommissie:	Prof. dr. P.B. Cliteur
	Prof. dr. P.A.L. Ducheine (Universiteit van Amsterdam)
	Prof. dr. U. Rosenthal
	Prof. dr. S. Van der Hof
	Dr. B.R. Rijpkema

Table of Contents

PART I: INTRODUCTION

1 General Introduction

"The Grid. A digital frontier. I tried to picture clusters of information as they moved through the computer. What did they look like? Ships? Motorcycles? Were the circuits like freeways? I kept dreaming of a world I thought I'd never see. And then, one day... I got in."[1]

On 25 February 1603, three Dutch ships with the Dutch East India Company (hereinafter: "V.O.C.") were sailing the straits of Malacca, between Indonesia and Malaysia. At dawn, the ships spotted the Santa Catarina, a galleon belonging to the Portuguese fleet. Upon this discovery, Admiral Jacob van Heemskerck, commander of the Dutch ships, decided to try to capture the Portuguese ship. After several hours of fighting, the V.O.C. ships came out victorious and seized the Santa Catarina, which was laden with products from China and Japan - including 1200 bales of Chinese raw silk and large amounts of Ming Chinese porcelain. The capture amounted to a prize so rich that it effectively increased the capital of the V.O.C. by 50%, thus enticing the Dutch shareholders to try to keep the prize, while the Portuguese demanded the return of their cargo.

The capture led to much discussion on the law of capture and a broader discussion on the applicability of the concept of State sovereignty to the seas.[2] At the time, Portugal claimed sovereignty over the Atlantic Ocean South of Morocco and over the Indian Ocean.[3] As was common practice during the age of discovery, Portugal sought to exercise its sovereignty over these waters by excluding all foreigners from entering, navigating or passing through them.[4] Although the Dutch Republic was at war with Portugal at the time of the capture, and although the V.O.C. possessed quasi-governmental powers such as the ability to wage war and claim territories, Van Heemskerck had not been authorized by the Dutch government to initiate the use of force.[5] Unhindered by this lack of authorization, the V.O.C. sought to keep the prize *post-facto* and called upon Dutch jurist Hugo Grotius (1583-1645) to draft a defence to persuade

[1] Tron: Legacy (2010). In the movie, Kevin Flynn, CEO of one of the largest technology companies in the world, creates a digital world in the 'TRON computer'. After accidentally entering this new digital world, he discovers that it contains many similarities and analogies to the physical world.
[2] *See* H. Grotius, The Freedom of the Seas, or the Right Which Belongs to the Dutch to Take Part in the East Indian Trade (hereinafter: "The Freedom of the Seas"), Translated by R. Magoffin, Introductory note by J. Scott (hereinafter: "Introductory Note to The Freedom of the Seas", New York, Oxford University Press (1916), p. v.
[3] *See* Scott, Introductory Note to The Freedom of the Seas, p. vii.
[4] *Id.*
[5] *Id.*

Dutch courts and international public opinion at large, of the legality of the capture.[6] It is in this context that Grotius wrote *De Jure Praedae* (*On the Right of Capture*), which laid the basis for *De jure belli ac pacis* (*On the Law of War and Peace*).[7]

Although *De Jure Praedae* was not made public during Grotius' lifetime (possibly because the need to persuade the Dutch courts was negated by their favorable ruling on the case in 1606), one chapter of it, Chapter XII, appeared in the form of an influential pamphlet in 1609, entitled *Mare Liberum* (*The Free Sea)*.[8] In *Mare Liberum*, Grotius formulated a new principle, based on natural law, which was aimed at providing an overarching theory of the legality of the V.O.C.'s conduct, namely that States could not claim sovereignty over the sea, as the sea was international territory,[9] and that all nations were hence free to use it for seafaring trade.[10] Although this principle stood in staunch contrast to the *mare clausum* (closed sea) policy as supported by the Portuguese, the *mare liberum* principle, as formulated by Grotius, offered a convincing legal theory on the applicability of State sovereignty to the seas.[11] Resultantly, the international community came to agree on the principle that State sovereignty over territorial waters needed to extend outward from terrestrial territory, and that it needs to be limited to what can be effectively controlled.[12] Another Dutch jurist, Cornelius van Bynkershoek (1673-1743), eventually provided a practical application of this principle by suggesting that this range of State sovereignty which extends outwards from terrestrial territory, be limited by the range of cannon fire – namely three nautical miles from a coast line (later extended to 12 nautical miles).[13] The rest of the seas came to be referred to as the 'high-seas' and were declared to lay beyond the limits of national jurisdiction and sovereignty.[14] Resultantly, the high-seas could henceforth be used as trade-routes to benefit all States, thereby challenging the structural

[6] *See* Scott, Introductory Note to The Freedom of the Seas, p. v-vii.
[7] *See* Scott, Introductory Note to The Freedom of the Seas, p. v-vi.
[8] *See* Scott, Introductory Note to The Freedom of the Seas, p. v, viii.
[9] *See* Grotius, The Freedom of the Seas, p. 11-60.
[10] *See* Grotius, The Freedom of the Seas, p. 61-64.
[11] *See* Scott, Introductory Note to The Freedom of the Seas, p. ix.
[12] 1962 Convention on the High Seas (hereinafter: "High Seas Convention"), 450 UNTS 11; 1964 Convention on the Continental Shelf (hereinafter: "Continental Shelf Convention"), 499 UNTS 311; 1964 Convention on the Territorial Sea and Contiguous Zone (hereinafter: "Territorial Sea Convention"), 516 UNTS 205; 1966 Convention on Fishing and Conservation of the Living Resource of the High Seas (hereinafter: "Fisheries Convention", 559 UNTS 285; 1982 United Nations Convention on the Law of the Sea (hereinafter: "UNCLOS"), 1833 UNTS 3. UNCLOS replaced the previous four conventions on the law of the sea.
[13] *See* C. Van Bynkershoek, *De Dominio Maris Dissertatio (Dissertation on the Ownership of the Sea)*, Translated by R. Magoffin, Introductory note by J. Scott, New York, Oxford University Press (1923). Although Van Bynkershoek formulated the "cannon shot rule", it was in fact the Italian Ferdinand Galiami who calculated this final range.
[14] Art 137(1) UNCLOS: "No State shall claim or exercise sovereignty or sovereign rights over any part of the [high seas] Area or its resources, nor shall any State or natural or juridical person appropriate any part thereof. No such claim or exercise of sovereignty or sovereign rights nor such appropriation shall be recognized.".

relationship between rich and poor countries that the *mare clausum* policy supported.[15] In later discussions, since the high seas were free to be explored and exploited by all, without State interference, they came to be referred to as the 'Common Heritage of Mankind'.[16]

In the centuries that followed the discussion on the sovereignty over the high seas, continued advances in technology allowed for the discovery of new spaces which, for all intents and purposes, had also been previously non-accessible and non-existent to Mankind. Similar to how large seafaring ships enabled the exploration and exploitation of the high-seas, so too did the ability to launch spaceships and manned spaceflight bring (the exploration and exploitation of) outer space into existence to Mankind. Similar to the high seas, the international community soon came to realize that the establishment of State sovereignty over outer space – including the moon and celestial bodies – would be undesirable, as it too would ostensibly continue to support a structural relationship between rich and poor countries.[17] Resultantly, international space law came to designate the domain of outer space too as part of the Common Heritage of Mankind.[18]

Currently, continued advances in technology are allowing for the exploration and exploitation of another new space; *cyberspace*. Similar to how the arrival of large sea- and spacefaring ships capable of traversing the high seas and outer space, has previously pushed Mankind's boundaries and motivated the international community to set out legal theories governing the high seas and outer space respectively, so too will the crossing of the digital frontier with the advent of the computer and internet motivate the international community to

[15] *See* Grotius, The Freedom of the Seas, at 1: "The delusion is as old as it is detestable with which many men, especially those who by their wealth and power exercise the greatest influence, persuade themselves, or as I rather believe, try to persuade themselves, that justice and injustice are distinguished the one from the other not by their own nature, but in some fashion merely by the opinion and the custom of mankind. Those men therefore think that both the laws and the semblance of equity were devised for the sole purpose of repressing the dissensions and rebellions of those persons born in a subordinate position, affirming meanwhile that they themselves, being placed in a high position, ought to dispense all justice in accordance with their own good pleasure, and that their pleasure ought to be bounded only by their own view of what is expedient.". These opening sentences of *Mare Liberum* set the stage for Grotius' argument against the structural relationship which the *mare clausum* policy supported and which the *mare liberum* policy contested, successfully.

[16] Art. 136 UNCLOS: "The Area and its resources are the common heritage of mankind".

[17] 1967 Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies (hereinafter: "Outer Space Treaty"), 610 UNTS 205, Agreement Governing the Activities of States on the Moon and Other Celestial Bodies (hereinafter: "Moon Treaty"), 1363 UNTS 3.

[18] Art. 1 Outer Space Treaty: "The exploration and use of outer space […] shall be carried out for the benefit and interest of all countries, irrespective of their degree of economic of scientific development, and shall be the province of all mankind […]", art. 2 Outer Space Treaty: "Outer space […] is not subject to national appropriation by claim of sovereignty […]", art. 11 Moon Treaty: "[t]he Moon and its natural resources are the common heritage of mankind […]".

set out a legal theory on how to govern cyberspace. Borders need to be drawn in the domain of cyberspace - both between and beyond States.

Therefore, pursuant to the most fundamental principle of political philosophy, State sovereignty, the main research question which needs to be answered in this dissertation, is:

Can social contract theory on State sovereignty be applied to the domain of cyberspace?

Asking this question immediately raises several additional questions. For example, if State sovereignty is defined as the sovereignty which a State exercises within the borders of a specifically delimited physical space, then how can such sovereignty extend to the non-physical domain of cyberspace? Does this sovereignty extend outward from the territory where the people in a State live - as it does with territorial waters - and thus connect to the physical cyber infrastructure located within a specific territory? Or, does this sovereignty perhaps follow the jurisdiction which States have over their citizens and corporations, regardless of their physical whereabouts? Or, inversely, are there parts of cyberspace which are to be regarded as naturally autonomous and thus not falling under the sovereignty of any States – as a common heritage of mankind? Or, alternatively, is cyberspace perhaps still just a *terra nullius*, waiting for someone to plant a flag and declare it as his own?

Additionally, asking these questions on the applicability of sovereignty to cyberspace brings some apparent issues to the fore. For one, similar to the high seas, cyberspace, with its inherently trans-boundary and anonymous nature, does not *prima facie* seem to comply easily with the Westphalian concepts of border divisibility and effective control. Hence, any legal theory on governing cyberspace needs to address the limited ability of States to actually declare digital borders and to divide cyberspace. Second, contrary to the space which Grotius was setting out a legal theory for, the space that this dissertation will set out a legal theory for has not always existed (leaving aside for a moment the question of whether or not cyberspace as a non-physical domain can be said to 'exist'). Since cyberspace is a man-made and non-physical space, it is unclear what its relation is with the territorial entity that is the State, nor, if we follow Grotius' reasoning of natural law, what its 'natural' place is in the world. Third, because its existence is relatively new and continues to be an emergent phenomenon – as can be seen in Appendixes 1-3 - cyberspace is not a domain in stasis. Rather, its constituting dimensions of

processing power, storage capacity and transmission speed grow and do so at an exponential speed. Hence, in order to avoid irrelevance upon completion, it will be required in this dissertation to make some general predictions about the direction in which cyberspace is heading.

A comprehensive legal theory on how to govern cyberspace needs to address the abovementioned questions and difficulties created by the abovementioned unique attributes of cyberspace. In the following chapters of this dissertation, I will attempt to provide such a theory.

Thereto, there are three main parts to this dissertation:

I. Introduction
II. Framework
III. Application
IV. Conclusion

Part I consists of Chapters 1 and 2 and it will contain a general introduction and a factual background which will answer the question of what the domain of cyberspace actually is. Part II consists of Chapter 3 and it will try to answer the question under which conditions States can claim sovereignty over a certain space pursuant to social contract theory. Part III consists of Chapters 4-6 and will combine the findings of Part I and Part II to try to answer the question of whether the conditions (as discussed in Chapter 3) are met in the domain of cyberspace (as discussed in Chapter 2). Finally, Part IV will contain a general summary as well as concluding observations and recommendations.

In Chapter 2, the dissertation will first provide the reader with a factual background containing the definition, delineation and delimitation of the domain of cyberspace. Thereto, this chapter will commence with setting out a historic overview of the emergence of the digital universe and of cyberspace thus far. Subsequently, it will explain the driving forces or ‘natural laws’ of the digital universe. Thereafter, the chapter will project the natural laws of the digital universe forward into the future. It will be argued in this chapter that as a result of the natural laws of the digital universe, that Mankind is about to enter the ‘Information Age’. At the end of the chapter, it will be clear to the reader what terminology will be used in the dissertation, what the domain of cyberspace encompasses and what its significance is to civilization and to the story of Mankind.

In Chapter 3, the dissertation will explore the conditions under which States can incorporate spaces as part of their sovereign domain. In order to do this, the chapter will start with the state of nature and explain how it naturally and logically leads to a war of all against all. Subsequently, the chapter will explain how from the state of nature, naturally and logically arises the laws of men, based on the agreement not to use of force against other participants to the agreement. Thereafter, it will be explained how from this agreement naturally and logically arises the need for a neutral arbiter who can enforce the agreement and why this entails the creation of a State which monopolizes the use of force. It will be argued that State sovereignty is dependent upon the monopolization of the use of force and that this entails establishing effective control over sovereign spaces – such as territorial-, water-, air- and cyberspace - so that it can protect the life, liberty and property of its citizens, both in their individual form as well as in their collective form as sovereign existence, political independence and territorial integrity.

In Chapter 4, the dissertation will focus on the first criteria of State sovereignty which is formulated in Chapter 3, namely the ability to establish and exercise effective control. If States cannot exercise effective control over operations which are conducted in a certain space – such as cyberspace - which are aimed against the life, liberty and property of citizens or against the sovereign existence, political independence or territorial integrity of the State, then any further discussion on sovereignty over cyberspace would be moot. Whether it is the high seas or cyberspace, States have to be able to exercise effective control in order for said space to fall within the sovereignty of said State. Thereto, the chapter will explore the extent to which States can exercise effective control over the domain of cyberspace, as defined, delineated and delimited in Chapter 2. It will argued that the so-called 'attribution problem' – which is caused by the anonymous nature of cyberspace - can be solved when it comes to cyber operations which meet the severity threshold for use of force and it will be explained why this dissertation focuses on operations conducted by States. At the end of the chapter, it will be concluded that States can, in fact, exercise effective control over the parts of cyberspace which fall within their sovereign domain, because cyber operations which meet the severity threshold for use of force cannot, by and large, be conducted with anonymity.

In Chapters 5 and 6, the dissertation will focus on the second criteria of State sovereignty which is formulated in Chapter 3, namely the protection of life, liberty and property as well as their collective form as sovereign existence, political independence and territorial integrity from force.

In Chapter 5, the dissertation will set out the legal and moral foundation for the concept of property. The chapter contains three main sections, dealing with how to attain ownership over objects, land and ideas, based on, respectively, *res nullius*, *terra nullius* and *data nullius.* Subsequently, it will be argued that, because in the Information Age value is mostly created in cyberspace, that States must consider the parts of cyberspace where their citizens create value, as part of the cyber territory of their respective States. Large-scale theft of intellectual property through cyber operations ought to hence be considered as severe as aggrandizement of (cyber) territory in violation of a State's territorial integrity by traditional kinetic means, such as through large-scale, state-sponsored (threats of) force (*e.g.*, artillery shelling, naval attacks, aerial strikes, *et cetera*).

In Chapter 6, the dissertation will discuss the relationship between Man and Machine. It will be argued that technology needs to be understood as an extension of the human body and, pursuant to an anatomy analogy, that critical infrastructures need to be regarded as extensions of the State body, with the infrastructures of energy, matter and information functioning as, respectively, the respiratory-, cardiovascular- and central nervous systems of the State. Given the symbiotic relationship between Mankind and technology and between the State and critical infrastructures, it will be argued that durable disruption of critical infrastructures through cyber operations ought to be considerd as severe as a blockade of a State by traditional kinetic means, such as through large-scale, state-sponsored (threats of) force (*e.g.*, artillery shelling, naval attacks, aerial strikes, *et cetera*).

Finally, Chapter 7 is the capstone of this dissertation. It will contain a summary of the different chapters, as well as concluding observations and recommendations.

2 Factual Background: The Domain of Cyberspace

"That's one small step for [a] man […]"[19]

2.1 Introduction

In order to answer questions on the applicability of sovereignty over the domain of cyberspace, we first have to define both *sovereignty* and the *domain of cyberspace*. Chapter 3 will define sovereignty. Chapters 5 and 6 will apply sovereignty to the domain of cyberspace. This current chapter will define, delineate and delimitate the domain of cyberspace.

Prima facie, we can assert that there are many different interpretations and perspectives we can take in order to describe what cyberspace is; we can take the *historical perspective*, whereby cyberspace ranges from the first mainframe computer to the latest personal computer; we can take the *geographical perspective*, whereby cyberspace can be found across the globe, in our deepest submarines, on Mars and even, in the case of Rover 1, outside of our galaxy; we can take the *computation perspective*, whereby cyberspace ranges from the smallest passive barcode to the largest active supercomputer; we can take the *data perspective*, whereby cyberspace ranges from our physical hard disks on our computers to our virtual storage in the cloud; we can take the *network perspective*, whereby cyberspace stretches wireless and cabled communications to all connected processors and storage; we can take the *personal perspective*, whereby cyberspace ranges from the physical gadgets in our pockets which we turn on in the morning, to our online lives which continue when we go to sleep at night; or we can take the *monitoring* perspective, whereby cyberspace ranges from the insight inside our bodies through pace-makers and insulin pumps, to the oversight overhead from the all-seeing eye in the sky through ever-persistent drones and satellites.

All of these perspectives, I will argue, are valid perspectives to take, but they are incomplete when it comes to dealing with the question of the applicability of sovereignty over cyberspace. In order to provide a solid foundation for the legal and philosophical theory presented in this dissertation, this chapter's focal point will be a thorough examination of the factual extent of cyberspace and the significance of cyberspace to Mankind. By doing so, this

[19] Astronaut Neil Armstrong famously describing his (and simultaneously, Mankind's) first step on the lunar surface, on 02:56:15 UTC July 20, 1969, 109:24:23hrs after the Apollo 11's liftoff from earth's surface at the Kennedy Space Center in Merritt Island, Florida, Earth.

chapter will provide an appropriate factual context in which the legal and philosophical discussion of this dissertation can take place. *Ex factis jus oritur.*

Thereto, the substantive part of this chapter will start in Section 2.2 with, as custom demands, a brief overview of the historical development of cyberspace from its inception up until the present day. It will contain a description of several important historical developments and it will also explain and define some of the terminology which will be used throughout this dissertation. In the sections thereafter, I will explain the significance of the digital universe and of cyberspace to the story of Mankind. As will be explained near the end of this chapter, without truly understanding this significance, it is not possible to properly apply the legal and philosophical theory of sovereignty to the domain of cyberspace. Thereto, Section 2.3 will first discuss the digital forces which shape the constituting dimensions of the digital universe, namely processing power, storage capacity and transmission speed. These forces, it will be argued, are 'natural laws' of the digital universe in a similar way to how the laws of physics shape the constituting dimensions of the physical universe. Subsequently, Section 2.4 will take these natural laws of the digital universe and project them forward into the future. As touched upon briefly in Chapter 1, the domain of cyberspace is a domain which is not in stasis. This section will therefore discuss the next developments of cyberspace, namely the internet of everyone and the internet of everything. After these developments have been described, the section will zoom out and look at the significance of these developments in the story of Mankind. In this section I will argue that with these new developments, Mankind is not just writing a new paragraph in Mankind's chapter on the Industrial Ages (as is often argued by commentators and observers), but rather, that we are writing an entirely new chapter of civilization as we are about to enter the Information Age. Finally, Section 2.5 will provide a summary of the chapter and place it in the context of the other chapters.

2.2 On the Historical Development of the Digital Universe

"*In the beginning was the command line*", started science historian George Dyson (1953) his wonderful account on the origins of the digital universe – thereby poetically describing the 'digital universe' as having been willed into being by a divine command.[20] In *Turing's Cathedral*, Dyson describes how, in late 1945, at the newly created Institute for Advanced

[20] *See* G. Dyson, Turing's Cathedral – The Origins of the Digital Universe (2012) (hereinafter: "Turing's Cathedral), p. xiii.

Study in Princeton, New Jersey, a small group of brilliant engineers and mathematicians under the direction of polymath John von Nuemann, willed the computer into being which would come to provide the numerical framework that would underpin almost all of our modern computing.[21] At the time, the group was tasked to build a computer which would be instrumental to the US government's race towards the creation of a hydrogen bomb.[22] The mathematicians themselves however, saw their project as the realization of a 'Universal Turing Machine'.[23] Such a machine, theorized by famous British mathematician Alan Turing (1912-1954) in his seminal paper *On Computable Numbers*, could be programmed to simulate the logic of any computation algorithm, as opposed to existing special purpose computers which could only compute specific algorithms.[24] This new computer could hence be used not just for the special purpose of simulating nuclear chain reactions, but also as a general purpose computer to compute any computable algorithm. In other words, the architecture of this computer had the potential to be turned into the computer sitting prominently on my desk, rather than the calculator lying hidden away in my drawer. As such, this computer, originally conceived to build the ultimate weapon of destruction, ended up also forming the legacy for the modern computer - the ultimate tool for creation.

Notably, this general purpose computer was the first computer to hold a static memory, meaning that it could store information on its memory chip (as opposed to previous external punch cards).[25] Dyson describes this rather poetically as the moment when a so-called *digital universe* came into being, a universe which could continue to exist (somewhat) independently from continued human input.[26] Except for a continuous supply of electricity and occasional repairs, a world of information came into being in which programs and viruses could, in some sense, be said to 'live'.[27]

Although there are as many authors who use different descriptions to describe this phenomenon as there are authors using different descriptions to describe terms such as god, love and beauty, and although the adjective 'digital' may not be applicable in the future for a

[21] *See* Dyson, Turing's Cathedral, p. ix.
[22] *See* Dyson, Turing's Cathedral, p. 216-221.
[23] *See* Dyson, Turing's Cathedral, p. ix "I am thinking about something much more important than bombs. I am thinking about computers – John von Nuemann, 1946".
[24] A. Turing, *On Computable Numbers*, Proceedings London Math Society, 230-265 (1937).
[25] *See generally* Dyson, Turing's Cathedral, p. 225-242.
[26] *Id.*
[27] *Id.*

variety of reasons,[28] for the purposes of this dissertation, the term digital universe will henceforth be used to describe the space which has been created by Mankind. The dimensions of this space are, as will be discussed in more detail in Section 2.3, processing power, storage capacity and transmission speed. At this point in this dissertation, it is however useful to first separate the term digital universe from two related and distinct (but often erroneously conflated) terms: *virtual space* and *cyberspace*.

Because, as stated above, many definitions of these terms exist, I will base my definitions of these and other terms on the Oxford Dictionary.

Virtual space comes from the field of virtual reality, which is defined by the Oxford Dictionary as: "*The computer-generated simulation of a three-dimensional image or environment that can be interacted with in a seemingly real or physical way by a person using special electronic equipment, such as a helmet with a screen inside or gloves fitted with sensors*".[29] Virtual reality in this reading refers to a simulation of a physical space with sensory experiences akin to the physical world. Although originally in the 80s and 90s (somewhat unimaginatively) thought of as the future of the digital universe, nowadays, virtual spaces are a small fringe of the digital universe. Although such simulated physical spaces may play a more important part in the digital universe of the future,[30] for the purposes of this dissertation, dealing with virtual space will only be done in passing. Such a physical approach to a 'space' is, as will be explained further down in this chapter, simply too literal for a non-physical, digital space.[31]

Cyberspace is distinct from both these previous categories because, contrary to the digital universe, it is mostly dependent on human input (direct and indirect[32]) without being a simulation of a physical space. It is defined in the Oxford Dictionary as: "*The notional*

[28] *See infra* Section 2.3. Besides digital computing, there are many new types of so-called 'unconventional computing' which are being developed. There are approaches based on physics (optical computing, spintronics, atomtronics, fluidics and quantum computing), chemistry (molecular computing), biochemistry (peptide computing and DNA computing), biological processes (neuroscience, cellular automata and amorphous computing) and approaches based on mathematics (analog computing, ternary computing, reversible computing, chaos computing, stochastic computing). Although some of these types of unconventional computing seem more promising than others, at this point in time, it is not clear which or if any of these types will be the winning approach for the near future or whether the current method of digital computing will remain prominent.

[29] Virtual Reality. In: *Oxford Dictionary*, available at: https://en.oxforddictionaries.com/definition/virtual_reality (accessed on 31st July, 2017).

[30] *E.g.* for the purposes of communication, education, entertainment.

[31] *See infra* Section 2.4.

[32] *See infra* Section 2.4. Currently most input of data and information in cyberspace is done more or less manually through direct human input. We are however seeing a trend whereby Mankind is developing sensors and machines which can input information more or less autonomously. Hence the term 'indirect input'. This input will quickly become the dominant input of information into cyberspace as we move towards the 'Internet of Things', which will be discussed in Section 2.4.

environment in which communication over computer networks occurs".[33] Cyberspace in this reading is the part of the digital universe which is the conceptual space which is functional to Mankind for the communication of data and information. When considering the relation between cyberspace and the digital universe, for the purposes of this dissertation, the digital universe will refer to the full space which is created by processing power, storage capacity and transmission speed and cyberspace will refer to the part of this digital universe where Mankind has created functional use. The digital universe is thus the vast world, which is mostly a wild wilderness and cyberspace is the part of this universe where Mankind has brought order and civilization - akin to the spaces which civilizations have captured and cultivated in the physical universe.[34]

Historically speaking, besides several important developments of *computation*, as discussed above, we can also discern several important developments of *connectivity*. Two important developments contain terms which need to be defined, namely the internet and the web.

The arrival of the *internet* is the first development and term which needs to be defined. The Oxford Dictionary defines it as: "*A global computer network providing a variety of information and communication facilities, consisting of interconnected networks using standardized communication protocols*".[35]Internet in this reading, refers to the communication infrastructure – both physical and digital – which connected the previously separate 'digital islands'. Pursuant to this Oxford Dictionary definition, this is when we could first speak of a singular digital space. Even though there are still parts of the digital universe which are not connected to the internet and even though there is some balkanization of the internet which makes referring to the internet in the singular as somewhat of a misnomer,[36] the overwhelming majority of the digital universe is in fact (inter)connected through the internet and I will treat it as such throughout this dissertation.

---

[33] Cyberspace. (2017). In: *Oxford Dictionary*, available at: https://en.oxforddictionaries.com/definition/cyberspace (accessed on 31st July, 2017).

[34] *See infra* Sections 5.3-5.4; *See generally infra* Chapter 5. In this chapter I discuss how the right to ownership is established over *res nullius*, *terra nullius* and *data nullius* by occupying and cultivating it into produced things, produced land and produced ideas, respectively. In other words, by taking these raw resources of raw materials, land and data and creating something new with them which adds additional, original value, the creator takes them out of the public domain and into the private domain in the sense of ownership. Mankind has thus established order and civilization in small parts of the universe and it has done the same with small parts of the digital universe.

[35] Internet. (2017). In: *Oxford Dictionary*, available at: https://en.oxforddictionaries.com/definition/internet (accessed on 31st July, 2017).

[36] *See infra* Section 2.4. In this section, the balkanization of the internet – which is mostly caused by religious and authoritarian entities - is discussed.

Subsequently, the next important development in connectivity was the arrival of the world wide web (www), or simply 'the web'. The Oxford Dictionary defines it as: "*An information system on the Internet which allows documents to be connected to other documents by hypertext links, enabling the user to search for information by moving from one document to another*".[37] The web thus brought a system of easily navigable interlinked hypertext documents, which created tremendous user value due to the simplified user interface of internet browsers (instead of the previous command screens which required users to memorize vast sets of complicated commands which had to be entered manually). Because of this simplicity, the internet spread beyond mere private individuals and started including companies and governments as well. Resultantly, we have moved beyond mere personal websites and started seeing professional and public websites and services as well.

In sum, this section has described several important historical developments as it relates to computation and connectivity, and it has defined several terms which will be used throughout this dissertation, namely; digital universe, virtual space and cyberspace. In the next sections, we will move from describing what cyberspace and the digital universe are, to describing what they will become and what this means. Any such description will require, as we will see, not just an overview of historical developments, but also some general predictions about future developments – lest the dissertation risks becoming obsolete upon completion. In Section 2.4 this chapter will discuss the newest developments of connectivity; the internet of everyone and everything. Before that, it is necessary to first explain briefly how individual information technologies, as the formative forces or 'natural laws' of the digital universe, shape it.

2.3 On The Natural Laws of the Digital Universe

In the previous section, we have seen that we have moved from an internet that was merely personal to one that is professional and public as well. In order to understand why we are now moving towards an internet of everyone and an internet of everything, we first have to discuss the information technologies which constitute the dimensions of the digital universe.

Information technology is defined in the Oxford Dictionary as "*The study or use of systems (especially computers and telecommunications) for storing, retrieving, and sending*

[37] World Wide Web. (2017). In: *Oxford Dictionary*, available at: https://en.oxforddictionaries.com/definition/world_wide_web (accessed on 31st July, 2017).

information".[38] For the purposes of this dissertation the term information technology will be used to describe the logic of the digital universe - similar to the way that physics describe the logic of the physical universe.[39] This logic can be explored ("study") or exploited ("use").[40] Individual information *technologies* constitute the dimensions of the digital universe, namely the dimensions of *processing power* ("retrieving information" with processors), *storage capacity* ("storing information" through sensors and memory chips) and *transmission speed* ("sending information" through cabled and wireless connectivity) of data and information.[41] Analogous to the way that the laws of nature determine the constituting dimensions of the physical universe, information technologies determine the constituting dimensions of the digital universe. They are its breadth, depth and height.

Many observers and commentators, from a variety of disciplines, have noted that since the birth of the digital universe, the different information technologies which constitute this universe – namely processing power, storage capacity and transmission speed - have displayed a certain level of predictability with regards to the development of their capabilities.[42] The digital universe, just as its physical counterpart, seems to be governed by a particular set of laws which can, to a certain extent, be predicted and described as 'natural laws'. Although the 'laws' of the digital universe are not as predictive as the laws of physics - such as gravity - they are reliable enough to base the predictions on which this dissertation uses. For the purposes of this dissertation, a classification is made into three constitution dimensions of the digital universe, namely; processing power, storage capacity and transmission speed, as well as three main trends which influence these dimensions, namely; acceleration, miniaturization and dematerialization.

The first trend of the digital universe is that the capabilities of the information technologies which make up the digital universe are increasing at an accelerating pace. There are many examples of this, but the most obvious, most well-known and arguably most important example, which will be used to illustrate and argue the point, is Moore's Law.[43]

---

[38] Information Technology. (2017). In: *Oxford Dictionary*, available at: https://en.oxforddictionaries.com/definition/information_technology (accessed on 31st July, 2017).
[39] Information and Communications Technology (ICT) is sometimes erroneously used as a synonym of Information Technology. In fact, ICT is more a specified term of IT, dealing specifically with (unified) transmission of communication, such as Voice over IP (VoIP).
[40] *See supra* note 38.
[41] *Id.*
[42] *See especially* R. Kurzweil, *The Singularity is Near – When Humans Transcend Biology* (2005) (hereinafter: "The Singularity is Near"), Chapter 2, p. 35-72; s*ee also generally* K. Kelly, *What Technology Wants* (2010), Chapter 8; *see also generally* K. Kelly, *The Inevitable* (2016), Chapter 10.
[43] *See* Appendix 3. The Natural Laws of the Digital Universe: Transmission Speed, Appendix 1. The Natural Laws of the Digital Universe: Processing power at p. 3.

Moore's Law was discovered in 1965 by Intel Corporation co-founder Gordon Moore (1929) and is most commonly understood to refer to the observation that the amount of calculations which can be performed by a computer chip per second for a 1000 dollars, doubles roughly every 18-24 months.[44] In other words, every 18-24 months, a consumer can reasonably expect to be able to purchase roughly double the amount of processing power for the same amount of dollars, or to be able to purchase the same amount of processing power for half the amount of dollars. The significance of this trend can hardly be overstated. Since many companies and industries rely heavily on processing power, these companies and industries benefit directly from the continually improving cost/performance of computer chips.[45] After all, not only can their existing work be done faster and cheaper, but they can also start doing work which had previously not been possible to do in a cost- or time-effective manner – such as analyzing large datasets. Any problem which can be translated into a digital problem, can hence be solved faster, at the rate of Moore's law and, as we will see in Section 2.4 on the future developments of the digital universe – such as the internet of things - more and more problems *are* therefore being translated into digital problems.[46] Also, because of the widespread knowledge of Moore's Law within companies and industries, companies and industries can anticipate the capabilities of the next generation of computer chips and can hence plan their business strategies accordingly.[47]

There are several important observations to make concerning this first trend of the digital universe. The first important observation to make is that this progress is exponential, not linear. A commonly used example to illustrate the counter-intuitiveness of exponential progression is the story of the inventor of the game of chess.[48] According to the legend, the mathematician who invented the game of chess, demonstrated his invention to the king of India.[49] The king was very pleased with the game because it conveyed to him many strategic

[44] *See* Appendix 1. The Natural Laws of the Digital Universe: Processing power, at p. 3. Originally, Moore's Law was conceived by Gordon Moore to refer to the observation that the number of transistors that could be fitted on an integrated circuit (through etching on a silicon chip) doubled every 18-24 months – which is closely connected to the price-reduction when it comes to transistor processing. Ray Kurzweil discovered that this law could be dated back to previous paradigms of computing as well.
[45] *See generally* Kurzweil, *The Singularity is Near*, p. 35-72.
[46] *Id.*
[47] *Id.*
[48] *See e.g.* R. Naam, *The Infinite Resource – The Power of Ideas on a Finite Planet* (2013) (hereinafter: "The Infinite Resource"), Chapter 19. Naam starts Chapter 19, called 'The Decoupler', with a retelling of the same story about the invention of the game of chess. In the chapter, Naam argues that Moore's Law on processing speed functions as a 'decoupler' of (infinite) economic growth from finite physical resources.
[49] *Id.*

and military lessons.[50] Being so pleased, he asked the inventor to name his prize for coming up with such a great game.[51] The mathematician asked for something seemingly innocuous: one piece of rice for the first square of the chessboard, a doubling to two for the second square, another doubling to four for the third square, *et cetera*, until doubling to the 64th square.[52] The king was very pleased with this offer, initially, and asked his treasurer to make the necessary arrangements.[53] Unbeknownst to the king at the time, this simple arithmetic exponential calculation ended up amounting to more rice than all of the assets of the kingdom could purchase.[54] Thus, according to the legend, the mathematician subsequently became the new king.[55] (Another version of the story ends with the more likely outcome of the mathematician being decapitated.) It is because of this exponential progress that the most popular household gaming computer anno 2010, the Playstation 3 (>83 million units sold), possessed more processing power than did the largest supercomputers which the world's superpowers wielded near the end of the cold war, just 20 years prior.

The second important observation to make concerning the trend of acceleration, is that even though the logic of exponential progression is very counter-intuitive to man - who has evolved in the physical universe where progress occurs nearly exclusively linearly[56] – it is in fact very common in the digital universe. Actually, it is the very way the constituting dimensions of the digital universe are formed. In other words, this acceleration does not apply just to computation power (although it influences many others), but also to storage capacity and transmission speed.[57] The result of these accelerations is that the digital universe - seemingly like its physical counterpart - is expanding.[58]

As Dyson noted concerning the speed of progress in the digital universe:

[50] *Id.*
[51] *Id.*
[52] *Id.*
[53] *Id.*
[54] *Id.*
[55] *Id.*
[56] Bacterial growth is a commonly known example of exponential growth in the physical universe, but it has been visible to Mankind only since the invention of the microscope – which is very recent in evolutionary terms. Arguably, *homo sapiens* as a biological species has had no evolutionary push to develop instinctive comprehension of exponential progression.
[57] *See infra* Section 2.3.
[58] *See supra* Section 2.2.

> "Time in the digital universe and time in our universe are governed by entirely different clocks. In our universe, time is a continuum. In a digital universe, time (T) is a countable number of discrete, sequential steps. […] To an observer in our universe, the digital universe appears to be speeding up. To an observer in the digital universe, our universe appears to be slowing down."[59]

As indicated above, besides acceleration, the digital universe is also subject to the trends of miniaturization and demassification.

Miniaturization of information technologies refers to the increasing capability of information technologies per unit of volume, weight, material, energy or other resource. In other words, over time, a specific information technology can reasonably be expected to attain roughly the same capability with a smaller footprint in the physical world or a larger capability with the same physical footprint. There are many examples of this, but the most obvious, most well-known and arguably most important example, which will be used to illustrate and argue the point, is Kryder's Law.[60]

Kryder's Law was discovered in 2005 by Seagate Corp. Senior Vice President of Research Mark Kryder (1943) and it describes the observation that the density of magnetic disk storage roughly doubles every 18 months.[61] In other words, every 18 months, a consumer can reasonably expect to be able to fit roughly double the amount of storage in the same amount of space – such as his pocket – or the same amount of storage in half the amount of space. The density with which information can be stored, increases, thus information can be fitted in a decreased physical space. This law - which exists almost entirely independent from processing power - progresses at an even faster pace than does processing power and it has a major influence on Mankind's ability to store and access vast amounts of data.[62] Moreover, this law does not just apply to storage density. The aforementioned Moore's Law, as it was originally formulated by Gordon Moore himself, described the doubling of the amount of transistors which could be fitted on a chip (which relates closely to the cost/performance of a chip, *i.e.* the more common and arguably more appropriate used definition of Moore's Law).[63] It is because

[59] *See* Dyson, Turing's Cathedral, p. x-xi.
[60] *See* Appendix 2. The Natural Laws of the Digital Universe: Storage Capacity, at p. 4.
[61] *Id*.
[62] *See generally* Kurzweil, *The Singularity is Near,* p. 35-72.
[63] *See generally* Kurzweil, *The Singularity is Near,* p. 35-72.

of this process of miniaturization that computers, which were originally stationed as mainframe computers in libraries and universities, have come into our homes as personal computers and can now be carried around in our briefcases and pockets as laptops and mobile phones, which can spend (most of) the day mobile and without (power) cords.

The third trend, dematerialization, refers to the elimination of materials altogether for certain functions.[64] There are many examples of this, but the most obvious, most well-known and arguably most important example, which will be used to illustrate and argue the point, Nielsen's Law.[65]

Nielsen's Law was discovered in 1998 by web usability consultant Jakob Nielsen (1957) and it describes how network connection speeds for high-end home users have doubled roughly every 24 months.[66] In other words, every 24 months, a consumer can reasonably expect to be able to have double the network speed for the same price or the same amount of network speed for half the price. The speed with which information can be transmitted thus increases and this has profound effects for the physical existence of many objects. Think for a second about our present-day most personal computation device; the mobile phone. Our mobile phones contain our (alarm) clocks, calendars, calculators, cameras, flashlights, mail correspondence, phones, phonebooks, voice recorders, notepads, maps, compasses, books, music players, remote controls, newspapers, navigational systems, keys, wallets and a suitcase worth of other items. Also, with the click of an icon, an additional warehouse worth of other items becomes instantly accessible through app stores. Additionally, any local device – whether it is a mobile phone or another type of computer - can have access to libraries worth of content, such as news, books, music, photos, videos, and other kinds of content, on a virtually limitless cloud, on top of which sits God-like computation power (which can be summoned without prayer). Although the mobile phone may not be a full replacement for all of these physical items, the prominence and existence of these physical items has certainly decreased and is continuing to decrease.[67] They have gone, and continue to go, from tangible to digital.[68] The most important contributing factor for many of these instances of dematerialization is the transmission speed with which local computers can communicate with other computers. The natural laws of the digital universe which deal with transmission speed thus possibly even bypass or override the need for local

[64] *See generally* Kelly, *What Technology Wants*, p. 57-72.
[65] *See* Appendix 3. The Natural Laws of the Digital Universe: Transmission Speed, at p. 5.
[66] *Id*.
[67] *See generally* Kelly, *What Technology Wants*, p. 57-72.
[68] *Id*.

processing power and storage capacity through, respectively, Moore's Law and Kryder's Law. Bits are replacing atoms and they are doing so at an exponential pace.

In this section we have thus far observed that the constituting dimensions of the digital universe – processing speed, storage capacity and transmission speed – seem to be subject to the trends of acceleration, miniaturization and dematerialization. The digital universe, it seems, is expanding and is doing so at an exponential pace. Before we can discuss what the consequences of these trends will be and where the digital universe is expanding towards, we will first have to assess whether it is likely that these trends are not just useful for hind-casting, but that they will also be useful for forecasting.

There are two main reasons proposed why the trends of acceleration, miniaturization and dematerialization could possible not continue to improve processing speed, storage capacity and transmission speed and that hence, the digital universe would stop expanding, namely;[69] natural laws of the digital universe are a self-fulfilling prophecy and they are hence not 'laws' in the true sense of the word and there are natural limits to the growth potential of the laws of the digital universe, due to the laws of physics.

These criticisms, I will argue briefly, are either largely untrue or mostly irrelevant for the purposes of this dissertation.

According to the first reason why the trends of acceleration, miniaturization and dematerialization could possible not continue to improve processing speed, storage capacity and transmission speed and that hence, the digital universe would stop expanding, the aforementioned progress in the constitutive dimensions of the digital universe is the result of the aformementioned targets which respective IT industries have set for processing power, storage capacity and transmission. Therefore, the progress which has been made has so far is thought to have been the result of a self-fulfilling prophecy.[70] Consequently, if industry leaders would have set different targets for their development cycles, these critics argue, these targets, either higher or lower, would have been the targets which would have defined the progress in

[69] *See generally* Kurzweil, *The Singularity is Near*, p. 35-72, 96-108. A third commonly heard criticism is that even though hardware increases in cost/performance, heavier software compensates these benefits. This so-called Wirth's Law (or The Great Moore's Law Compensator), states that even though computers have gotten faster, the boot-up time of software programs like Microsoft Word has not improved (or has even worsened). Given that this criticism implicitly acknowledges increases in computation capability (but subsequently applies flawed logic by assuming this should have functional results to end-users, regardless of computation increases), this criticism is not discussed here.

[70] *See generally* Kurzweil, *The Singularity is Near*, p. 35-72, 96-108.

the constitutive dimensions of the digital universe.[71] *Prima facie* there certainly seems to exist some element of truth to this criticism. After all, the natural laws of the digital universe have often received their very names from the people who have formulated these laws and these were often people at senior level positions of industry-leading companies. Even though these positions on the one hand made them expertly capable in making their respective predictions, on the other hand, their positions also often included the responsibility for billion dollar R&D budgets. These positions and responsibilities certainly also enabled them to execute on their own predictions, because they were able to place their predictions on the roadmaps of their respective companies and industries. Although there certainly exists some element of truth to this argumentation, there are several arguments which counter this criticism and which seem largely convincing. The first argument is the observation that such a self-fulfilling prophecy would not actually change the end-result in and of itself.[72] In other words, although it is true, it is irrelevant to the end-result. As long as companies and industries maintain their existing predictions, then the consumers of their products can consume predictably improved products. Moreover, even if this observation is ignored, there is an even more important counter-argument to this criticism. Ray Kurzweil - who has formulated a comprehensive unified theory of the predictability of progress of (information) technology the likes of which in scope can be best compared to Charles Darwin's comprehensive unified theory of biology - has pointed out that Moore's Law has actually not only held true since its inception by Gordon Moore in 1965, but even prior to that.[73] In other words, progress in processing power was already taking place according to Moore's Law before Moore coined the term and before he was even born.[74] It is important to recognize that, throughout the age of computing, there have been different paradigms of computing technologies. The paradigm in computing in which Von Neumann's team build the first computer to hold a static memory was in the paradigm of vacuum tube computing.[75] Even though the paradigm of vacuum tube computing was in many ways the first modern type of computing, it was preceded by two earlier paradigms of computing.[76] Vacuum tubes were hence the third paradigm of computing, with electromechanical- and relay computing being the respective first and second paradigms.[77] Although computers of these two types of computing could not hold a static memory, which is required for general purpose

[71] *See generally* Kurzweil, *The Singularity is Near*, p. 35-72, 96-108.
[72] *Id*.
[73] *Id*.
[74] *Id*.
[75] *See* Appendix 1. The Natural Laws of the Digital Universe: Processing power, at p. 3.
[76] *Id*.
[77] *See* Appendix 1. The Natural Laws of the Digital Universe: Processing power, at p. 3.

computing, they could perform many basic special purpose types of computing. After the paradigm of vacuum computing came the fourth paradigm of computing, transistor computing, and the fifth and current paradigm of computing, integrated circuit computing.[78] Notably, Moore's law has held true consistently not just during the current paradigm of integrated circuit computing, for which the law was formulated, but also during the four paradigms of computing which preceded both integrated circuits and Moore's prediction, dating back even to the 19th century.[79] In this sense, it seems that Moore's Law was not merely coined or created by Gordon Moore, but rather, that it was discovered.[80]

According to the second reason why the trends of acceleration, miniaturization and dematerialization could possible not continue to improve processing speed, storage capacity and transmission speed and that hence, the digital universe would stop expanding, the digital universe is inherently dependent upon and limited by the physical universe.[81] Hence, limits to the laws of nature will undoubtedly be reached at some point, especially when dealing with exponential growth curves.[82] The amount of matter and energy in the physical universe which can be used to build information technologies is simply finite.[83] Critics therefore pose that information technologies will have to run into some inherent limits because of the laws of physics.[84] For example, Moore's Law, in its original formulation, described the doubling of the amounts of transistors which could be fitted on an integrated circuit (which is closely related to the cost/performance of a chip). Since this entailed the increasingly shrinking size of transistors, some natural limits would have to be reached at some point. After all, when transistors would reach the single digits in nanometers, a limit would have to have been reached, given that integrated circuits are not physically able to distinctly carry voltage at that scale, which is the prerequisite for chips to communicate and compute. Ostensibly, this criticism has a *prima facie* plausibility. However, given the more commonly understood definition of Moore's Law as cost/performance in computation, as described previously in this section, the presumptions of both integrated circuits and shrinking size in the abovementioned limitation can be excluded. Again, integrated circuits could stop getting smaller, but their cost/performance could still improve exponentially in the computing paradigm of integrated circuits through new software

[78] *Id*.
[79] *Id*.
[80] *See generally* Kurzweil, *The Singularity is Near*, p. 35-72.
[81] *Id*.
[82] *Id*.
[83] *Id*.
[84] *Id*.

methods such as parallel, distributed or cloud computing. Also, currently, we are in the fifth paradigm of computing, the paradigm of integrated circuit computing. The IT industry is investing heavily in possible new paradigms of computing.[85] Since these methods have much larger theoretical capabilities, the end of Moore's Law is likely to be a far into the future. Physicists Lawrence Krauss and Glenn Starkman calculated that it would take at least multiple more centuries before Moore's Law will run out of steam.[86] This dissertation deals with mere decades. Also, as we have seen in earlier in this section, even when one of the constituting dimensions of the digital universe would no longer expand – such as processing power - the other dimensions could continue unhindered and possibly negate or bypass the need for the other dimension to continue. For example, even if processing power in a mobile device would not continue to improve, increased transmission speeds could outsource the processing to cloud computing which does not face the same physical restrictions to the same degree. Regardless, the predictions in Section 2.4 are based on improvements in processing power, storage capacity and transmission speed which are almost certain. Actually, most of the predictions in this dissertation are actually already almost possible and feasible with present day technology. Their adoption is more a measure of finding the right business models, marketing, regulatory approval and software rather than of continued technological development in hardware.

Before we will project the laws of the digital universe forward into the future and discuss the internet of everyone and the internet of everything, I want to briefly discuss how it is possible that information technologies keep improving at an exponential rate.

As several commentators and observers have noted, there is something fundamentally different between information technologies and other technologies.[87] As Kevin Kelly points out, all complex inventions are basically comprised of a combination of materials, energy and information.[88] The first two of these are largely limited by natural laws, whilst the latter is only limited by natural laws to a very small degree. You cannot keep adding materials and energy to most inventions, because you will quickly start racking up costs – both because the marginal costs per product increase accordingly and because both materials and energy are finite resources which increase in price the more they are nearing depletion. Information on the other

[85] *See supra* note 28.
[86] *See generally* L. Krauss, G. Starkman, *Universal Limits on Computation* (2004).
[87] *See especially* Kelly, *What Technology Wants*, p. 269-346.
[88] *Id*.

hand can be stacked largely without stacking additional costs.[89] Once an idea about how to combine materials and energy has been invented, the idea can be copied at next to zero marginal costs.[90] The marginal costs of building another car are comprised of great material costs in metals and the great energy costs which are required to process these metals into the shape of a car. The marginal cost in materials and energy for building another chip which processes, stores or transmits data are more or less negligible. Copying a car is expensive. Copying an idea is not. In this sense, information is, in the words of Ramez Naam, an 'infinite resource'.[91] Consider the metaphor by endogenous growth theory economist and Chief Economist at the World Bank, Paul Romer, quoted from Naam's *The Infinite Resource*:

> *"Imagine you wake one morning, refreshed from sleep, hungry for a simple but delicious meal or scrambled eggs, toast, and orange juice. But inexplicably, instead of scrambling the eggs, toasting the bread, and juicing the oranges, you find yourself forcing the eggs into the toaster, mashing the bread against the juicer, and attempting to crack oranges into the frying pan. How enjoyable would your breakfast be?*
>
> *This thought experiment (is like many thought experiments) absurd, but it also illustrates the importance of recipes (the way we manipulate and combine resources) vs. ingredients (the raw materials we begin with). The scrambled orange, toasted eggs, juiced bread breakfast starts with the same raw materials as the more conventional scrambled eggs, toasted bread and juiced oranges breakfast. It adds the same amount of energy (supplied in the toaster, the range heating up the frying pan, and the muscle power in moving and mashing the ingredients). Yet somehow, with the same ingredients, the two recipes don't produce equivalent results. The way the ingredients are put together matters."*[92]

When it comes to information technologies, their cost is almost entirely formed by the invention of their recipe, not by their raw ingredients. They are hence a product of human resources, not

[89] *See generally* Kelly, *What Technology Wants*, p. 269-347: "Complex inventions stack up information rather than atoms.".
[90] *Id*.
[91] *See generally* Naam, *The Infinite Resource*.
[92] *See generally* Naam, *The Infinite Resource*, Chapter 8.

of natural resources. They are almost entirely comprised of information, not of materials and energy. Even though information technologies are just tiny chips, they are the result of big ideas and of billions upon billions of dollars invested in R&D for trial and error, experimentation, refinement, and scientific investigation, in order to arrange cheap raw materials just a little bit better. Fundamentally, information technologies are ideas materialized. Because each additional unit (processor, chip, sensor) is so cheap to build after a new design idea has been discovered, once a certain development cycle has been finished, the resulting new product can be scaled up without much additional costs (besides marketing and distribution). Hence, they are subject to the laws of abundance, not the laws of scarcity to which most other technologies are subject.

In sum, this section has explained that there are three main trends which shape the constituting dimensions of the digital universe, namely the acceleration, miniaturization and demassification of the information technologies of processing power, storage capacity and transmission speed. The digital universe is expanding. This section has also argued that why it is safe to assume that these trends will continue and that the digital universe will hence continue to expand into the future. The next section will project these trends forward into the future and discuss two important future developments, namely; the internet of everyone and the internet of everything.

2.4 On the Future Development of the Digital Universe

In the previous section, we have seen that pursuant to the trends of acceleration, miniaturization and dematerialization the constituting dimensions of the digital universe of processing power, storage capacity and transmission speed keep expanding at an exponential pace and that this is likely to continue into the future. This section will project these trends forward into the future and describe where the digital universe is expanding towards. Seemingly, the digital universe is expanding into or merging with, the physical universe. As computer chips are increasingly shrinking in size and cost, whilst also increasing in capacity, they will find new applications and new adopters – thereby causing the physical world to become increasingly connected to and intertwined with, the digital world. For the purposes of this dissertation, a broad distinction will be made into two main developments of this expansion of connectivity; the increasing connectedness of *people* and the increasing connectedness of *things*.

The increasing connectedness of people and things can both be subdivided in the breadth and depth of those people and things connected, with the breadth referring to the amount of people or things connected and the depth referring to the intensity of their connectivity. In other words, the first category deals with the quantitative expansionist trend and the latter category deals with the qualitative expansionist trend. The increasing depth, or intensity, of connectivity can be recognized in all aspects of our daily lives. Initially, Mankind used to plug into cyberspace through large mainframe computers in libraries and universities. Subsequently, with the decreasing size and increasing cost/performance of computers, the personal computer brought access to cyberspace into our homes. Relatively soon thereafter, computers came in a format which allowed them to be carried around throughout the day in briefcases and even in our pockets, connecting us from the moment we when we wake up in the morning, until the moment when we go to sleep at night. Currently, we still carry our computers around and hold them to our ears or lines of sight - which signifies the absence of our mental presence from the physical world and into the world of information. In the future however, this distinction between the physical and digital worlds may very will diminish further or vanish altogether when our computers become wearable (and, if the promise of trans-humanism will hold true, someday, even implanted internally). Add to this the aforementioned products and services which have already moved or continue to move into cyberspace and we can quickly recognize the sheer depth, or intensity, of connectivity in our daily lives.

The increasing breadth, or amount of *people* connected can be best explained by Eric Schmidt and Jared Cohen, respectively executive chairman and director of ideas at Google. Their book *The New Digital Age – Reshaping the Future of People, Nations and Business* has been lauded by some of the most noted businessmen, scientists and politicians – including Bill Clinton, Henry Kissinger, Michael Hayden and Elon Musk.[93] In the book Schmidt and Cohen predict that the internet is poised to spread truly globally and connect five billion new minds to cyberspace within the next decade (2013-2023).[94] The reasons for this predicted spread are clearly manifold, ranging from entertainment value to political empowerment. Schmidt and Cohen however point to the economic argument as the most important reason.[95] As computers such as mobile phones become cheaper, more powerful and smaller pursuant to the trends and laws mentioned in Section 2.3, they argue, advantages and benefits of computing can be

[93] *See* E. Schmidt, J. Cohen, *The New Digital Age – Reshaping the Future of People, Nations and Business* (2013) (hereinafter: "The New Digital Age").
[94] *See* Schmidt, *The New Digital Age*, p. 4-11.
[95] *Id*.

attained at a cost-effective price for even the world's poorest.[96] Farmers on land as well as fishermen at sea can access weather forecasts or blue-prints of best practices to increase their respective yields and they can allocate their increased yields to the markets when and where they are most valuable.[97] Since the value of these increased efficiencies is easily larger than the cost of this access, Schmidt and Cohen argue, the adoption of computers, and hence the expansion of cyberspace, is more or less unavoidable.[98]

Schmidt and Cohen have noted that the expansion of cyberspace can be observed globally and, by and large, transcends differences in culture, politics or wealth.[99] States therefore, they observe, are consistently and predictably moving towards increasing connectivity. In this regard, they distinguish three categories of connectivity. There are the hyper connected states – such as Finland, Israel, and Sweden - which are heavily dependent on cyberspace for personal-, private- and public sector activity. Second, there are the partially connected states - such as Côte d'Ivoire, Guinea, Kyrgyzstan, and Pakistan - where authoritaritative governments are starting to experience the costs of having an increasingly connected people.[100] Third, there are the connecting states – such as Cuba, Burma and Yemen – where connectivity is still nascent and where both governments and citizens are still testing their desire to connect to cyberspace.[101] Even this latter category, which Schmidt and Cohen dub *connecting* states, signifies the direction cyberspace is heading; towards an ever-persistent, ever-present and very intimate connection everywhere with everyone.[102]

Although the expansion of cyberspace applies to nearly all places, there is an exception to this rule which, as the saying goes, proves it. Satellite imagery of North Korea at night shows cities blackened by the push-back against modernity and demonstrates that progress can indeed be held back - albeit temporarily. As Schmidt and Cohen have pointed out however, *grosso modo* the trend clearly points forwards and towards increasing connectivity.[103] While periodically and locally the trend may be to move slower or to possibly grind to a halt altogether,

[96] *Id*.
[97] *See* Schmidt, *The New Digital Age*, p. 14-18.
[98] *Id*.
[99] *See* Schmidt, *The New Digital Age*, p. 14-18, 83-96.
[100] *See* Schmidt, *The New Digital Age*, p. 83-96.
[101] *Id.*
[102] *Id.*
[103] *Id.*

actually going backward is practically non-existent.[104] As Chapter 6 on critical infrastructure will explain, there are clear reason as to why going backwards is practically non-existent.[105]

One caveat to note is that cyberspace may however not turn out to be one truly unified global space. The notorious examples of halal-internet in Iran and other Islamic places, kosher internet in orthodox Jewish places and the great firewall of China and other such ventures by authoritarian States will entail some sort of balkanization of cyberspace, with digital borders becoming more pronounced – albeit it more regionally than nationally and although these digital borders will most likely be highly porous.[106] However, Schmidt and Cohen predict that *grosso modo* people, organizations and states seem to be moving towards a more or less single cyberspace.[107]

Besides people, more and more *things* will also cross the digital frontier and come online. Similar to with people, for things this also will take place both in breadth and depth. Kevin Ashton, co-founder of the Auto-ID Center at the Massachusetts Institute of Technology, has coined the coming online of things as the *Internet of Things* (hereinafter: "IoT"). Ashton wrote in 2009:

> "*Today computers—and, therefore, the Internet—are almost wholly dependent on human beings for information. Nearly all of the roughly 50 petabytes (a petabyte is 1,024 terabytes) of data available on the Internet were first captured and created by human beings—by typing, pressing a record button, taking a digital picture or scanning a bar code. Conventional diagrams of the Internet ... leave out the most numerous and important routers of all - people. The problem is, people have limited time, attention and accuracy—all of which means they are not very good at capturing data about things in the real world. And that's a big deal. We're physical, and so is our environment ... You can't eat bits, burn them to stay warm or put them in your gas tank. Ideas and information are important, but things matter much more. Yet today's information technology is so dependent on data originated by people that our computers know more*

[104] *Id.*
[105] *See generally* Chapter 6. In short, societies adapt to and are built around critical infrastructures. Therefore, a nicety invariable develops into a necessity. Especially with connectivity to the internet, infrastructures, due to their communicative nature, become dependent upon continued access to the internet.
[106] *See* Schmidt, *The New Digital Age*, p. 83-96.
[107] *Id.*

about ideas than things. If we had computers that knew everything there was to know about things—using data they gathered without any help from us—we would be able to track and count everything, and greatly reduce waste, loss and cost. We would know when things needed replacing, repairing or recalling, and whether they were fresh or past their best. The Internet of Things has the potential to change the world, just as the Internet did. Maybe even more so."[108]

Ashton recognizes, rightly, that an internet of only people and ideas, although already providing tremendous value (something which he arguably patronizes slightly), is nothing compared to an internet which includes data and information derived from things as well. Things are what satisfy our most basic physiological needs at the bottom layers of Maslow's pyramid – such as air, food, water, clothing, shelter and transportation.[109] When more things become increasingly connected to cyberspace - by taking advantage of increasingly powerful, cheap and small sensors, chips, and (wireless) connectivity – a nervous system can be cast over the physical world which captures increasing amounts of data from the physical world. Subsequently, this data can be mined for nuggets of valuable information on how to improve the efficiency of the material and energy resources used for the production of goods and for the providing of services. The potential applications for the IoT are tremendous and so is the value that it can deliver to Mankind. For example, agricultural fields could become aware when and where water, fertilizer and pesticides need to be applied, instead of periodically flooding the entire field with them; data about mining activity could be mined to make scientific guesses about where to dig for natural resources next, instead of digging away mountains in a trial- and error manner; and the logistics of people, materials, energy and information could be directed along the channels with the most free capacity, instead of getting stuck in congestion on roads, power- and information lines. All of this results in an optimization in the use of natural resources and increases in productivity and efficiency.

As we go from communication between private persons, professionals and the public sector to communication between these private and public entities with things, as well as communication among things, this increasing connectivity of things to the digital universe and with cyberspace (the captured and cultivated parts of the digital universe) will have not just an

[108] K. Ashton, *'That 'Internet of Things' Thing'*, RFID Journal, July 22, 2009.
[109] *See* A. Maslow, A Theory of Human Motivation, Psychological Review 50, at 370-396.

evolutionary effect on civilization, but a revolutionary effect. According to Erik Brynjolfsson and Andrew McAfee, respectively professor and associate director at the Massachusetts Institute of Technology, the expansion of the digital universe and cyberspace into the world of things can be best understood as a third industrial revolution, after the earlier industrial revolutions caused by the advent of the steam-engine and electricity.[110] To note the impact of this development, consider the apt description historian Ian Morris used to describe the impact of the first industrial revolution. Morris commented: "[the first industrial revolution] made mockery of all that had gone before.".[111]

With the first two industrial revolutions, the advent of the steam engine and electricity allowed Mankind to tap into the accumulated energy resources which had been deposited in the fossil fuel bank for millions of years. It enabled Mankind to attain the same amount of physical power output with drastically fewer people, resulting in tremendous wealth and prosperity, as well as surpassing and replacing the previous agricultural revolution.

Similarly, according to Brynjolfsson and McAfee, with the third industrial revolution, the advent of computers and the internet, and the expansion of the digital universe and cyberspace into the physical world, will allow Mankind to tap into *information* resources which had previously been inaccessible.[112] It will allow Mankind to attain the same amount of mental power with drastically fewer people, resulting in tremendous wealth and prosperity, as well as surpassing and replacing the previous industrial revolutions.

Besides Brynjolfsson and McAfee, many others have also tried and continue to try to describe the importance of the internet of everyone and everything to Mankind and to do so in terms of industrial terminology. For example, Klaus Schwab, founder and executive chairman of the elite World Economic Forum, has dubbed this process 'The Fourth Industrial

---

[110] *See generally* E. Brynjolfsson, A. McAfee, *Race Against the Machine – How the Digital Revolution is Accelerating Innovation, Driving Productivity, and Irreversibly Transforming Employment and the Economy* (2011) (hereinafter: "Race Against the Machine"), Chapter 5: "History has witness three industrial revolutions, each associated with a general purpose technology. The first, powered by steam […] allowed huge and unprecedented increases in population, social development, and standards of living. The second, based on electricity, allowed these beneficial trends to continue and led to a sharp acceleration of productivity in the 20th century. […] The third industrial revolution, which is unfolding now, is fuelled by computers and networks." (emphasis added)

[111] *See* I. Morris, Why the West Rules –- For Now – The Patterns of History, and What They Reveal About the Future (2010) (hereinafter: "Why the West Rules -- for Now"), p. 582-623.

[112] *See generally* Brynjolfsson, *Race Against the Machine*, Chapter 5; *see also generally* Section 5.4.

Revolution',[113] whereas Marco Annunziata, Chief Economist at General Electric, has dubbed it 'The Industrial Internet'.[114]

The internet of everyone and everything will surely be revolutionary, but, according to the present writer, Brynjolfsson and McAfee, Schwab and Annunziata are all grossly underestimating its significance. A closer examination of the definition of this new revolution is in order.

According to the commonly used three-sector theory for describing economic activity, devised by Alan Fisher, Colin Clark and Jean Fourastié in the 1930s, economies can be divided into three sectors of activity: extraction of raw materials (primary sector), manufacturing of goods (secondary sector) and providing of services (tertiary sector).[115] According to this theory, the primary sector includes agriculture, forestry, fishing, drilling and mining; the secondary sector includes construction and manufacturing; and the tertiary sector includes research & development, professional services (legal, financial, tax, accounting and business consultancy), support services (human resource management and facility management), customer relationship management (public relations, marketing, sales and customer support), healthcare services (physical- and psychological), trade and retail, logistics, energy, (information and) communications technology, media and entertainment, art and design, education, public services and leisure (hospitality and wellness).[116]

Grosso modo, these three sectors deal with, respectively; matter, energy and information in order to increase economic output. In other words, the primary sector extract more raw materials, the secondary sector uses energy to process these raw materials into higher value products and the tertiary sector increases economic output through ideas about the optimal allocation of resources or through the creation of new intellectual products.

The first two industrial revolutions increased the productivity of people in the primary sector (*e.g.* with farming machines) and, later on, in the secondary sector (*e.g.* with factory

[113] *See generally* K. Schwab, *The Fourth Industrial Revolution* (2016). Schwab describes three megatrends which, when taken together, create, what he calls, 'the fourth industrial revolution'. Besides the digital trend as discussed in this section, Schwab also describes physical (autonomous vehicles, 3D printing, advanced robotics and new materials) and biological trends (DNA reading and writing).
[114] *See* General Electric, *available* at: https://www.ge.com/digital/industrial-internet (accessed on 31st July, 2017). The industrial internet refers to the application of the IoT to traditional industrial machines. By analyzing the data coming from these machines, companies can make their operations more efficient and make better strategic decisions.
[115] *See* J. Fourastié, *The Great Hope of the Twentieth Century*.
[116] *See* Fourastié, *The Great Hope of the Twentieth Century*.

machines), to allow people to move up the economic ladder, up the Maslow pyramid, into the tertiary sector and away from the dull, dirty and dangerous work. However, whereas these earlier revolutions brought Mankind physical power, the current revolution will bring it mental power. Just as the steam engine and electricity slowly but surely came to influence all aspects of our society so too will computers and the internet.

However, Kelly points out that contrary to the first two industrial revolutions of steam and electricity, on a fundamental level, the current revolution of computers and the internet does not deal with matter and energy, but with information.[117] It extracts and processes data - not materials and energy - in order to find valuable nuggets of information on how to do things more effectively and efficiently or how to do entirely new things.[118] Consequently, although this current revolution is also expected to increase the productivity in the primary sector (*e.g.* with smarter farming systems) and secondary sector (*e.g.* with smarter factory systems), its impact will be most noticeable in the tertiary sector – the sector dealing with information as its core-business.[119] Kelly therefore considers referring to the current revolution as an *industrial* revolution, as a miscategorization.[120] Instead, it is more appropriate to take a longer view of history and to note that, previously, Mankind has progressed from ages which are appropriately commonly referred to with materials, such as stone, bronze and iron; to ages commonly referred to with energy, such as steam, electricity and oil – referring respectively to hunter/gatherer, agricultural and industrial civilizations. Currently however, at the beginning of the 21st century, we are transitioning into an age in which increased *information* - as opposed to matter or energy -, is the most formative force of civilization.[121] Therefore, I will refer to the current age as the *Information Age*.

The gravity of the arrival of the Information Age can hardly be overstated and, without properly understanding and appreciating the gravity of this new age we are living in, a suitable legal theory on the governance of cyberspace cannot be set out - as will be made clear in Chapters 5 and 6 on intellectual property and critical infrastructure. The new age we are entering is not just another industrial age as a new section in Mankind's chapter on the Industrial Ages, but rather, it is an entirely new chapter of civilization, as revolutionary, unique and grand as

[117] *See generally* Kelly, *What Technology Wants*, p. 57-72.
[118] *Id.*
[119] *Id.*
[120] *Id.*
[121] *Id.*

our previous chapters on our hunter/gatherer, agricultural and industrial ages. We are writing a new chapter in the book of life and we are entering a new age; the *Information Age*.

2.5 Conclusion

On 20 July 1969, at 20:18, the spaceship Apollo 11 launched to transport its crew to the moon's surface. As it passed the clouds - where previous generations of religion and superstition thought Gods to reside and where future generations of science and technology will let their data reside - it was guided by one of the most powerful supercomputers at the time. This computer - which was the pinnacle result of the multi-decade all-out existential competition in science and technology between the two superpowers at the time, the US and the USSR - was vastly inferior to the computers we now all carry around everywhere all the time, at a fraction of the cost and size, and with a magnitude more power in processing power, storage capacity and transmission speed.

Six hours after launch, on July 21, at 02:56 UTC, Neil Armstrong (1930-2012) descended the ladder of the Apollo 11 to be the first person to set foot on a celestial body in outer space and spoke the famous words: "That's one small step for [a] man, one giant leap for Mankind". Similarly, now that we are leaving our first digital footprints, we are also taking a giant leap for Mankind into the digital universe, the accompanying exploration and exploitation of which has only just begun.

In this chapter I have discussed several important past developments of computation and connectivity as well as several future developments. Because of the trends of acceleration, miniaturization and dematerialization which shape the constituting dimensions of the digital universe of processing power, storage capacity and transmission speed, we are about to connect everyone and everything as we, as Mankind, are about to write the next chapter in our collective story and enter the Information Age.

The next chapters will discuss the fundamental principles and rules of State sovereignty and apply them to the parts of the digital universe which we have captured and cultivated. In other words, it will apply the fundamental principles and rules of State sovereignty to the domain of cyberspace to see if they still apply in the Information Age.

Chapter 3 will commence with setting out the legal theory for sovereignty and will argue that sovereignty over spaces arises from the effective control over such spaces through the

protection of citizens from force against life, liberty and property – both in their individual form as well as in their collective form as force against sovereign existence, political independence and territorial integrity. Subsequently, Chapter 4 will deal with the effective control part of the theory as set out in Chapter 3. Thereafter, Chapters 5 and 6 will deal with the protection of life, liberty and property aspect of the legal theory of State sovereignty as set out in Chapter 3. Chapter 5 will deal with intellectual property in the Information Age and will argue that large-scale theft of intellectual property needs to be regarded as severe as conquest of (cyber) territory. Chapters 6 will thereafter deal with infrastructures of matter, energy and information and will argue that durable disruption to these critical infrastructures needs to be regarded as severe as a territorial blockade.

PART II: FRAMEWORK

NOW this is the Law of the Jungle — as old and as true as the sky;
And the Wolf that shall keep it may prosper, but the Wolf that shall break it must die.

As the creeper that girdles the tree-trunk the Law runneth forward and back —
For the strength of the Pack is the Wolf, and the strength of the Wolf is the Pack.

Wash daily from nose-tip to tail-tip; drink deeply, but never too deep;
And remember the night is for hunting, and forget not the day is for sleep.

The Jackal may follow the Tiger, but, Cub, when thy whiskers are grown,
Remember the Wolf is a Hunter — go forth and get food of thine own.

Keep peace withe Lords of the Jungle — the Tiger, the Panther, and Bear.
And trouble not Hathi the Silent, and mock not the Boar in his lair.

When Pack meets with Pack in the Jungle, and neither will go from the trail,
Lie down till the leaders have spoken — it may be fair words shall prevail.

When ye fight with a Wolf of the Pack, ye must fight him alone and afar,
Lest others take part in the quarrel, and the Pack be diminished by war.

The Lair of the Wolf is his refuge, and where he has made him his home,
Not even the Head Wolf may enter, not even the Council may come.

The Lair of the Wolf is his refuge, but where he has digged it too plain,
The Council shall send him a message, and so he shall change it again.

If ye kill before midnight, be silent, and wake not the woods with your bay,
Lest ye frighten the deer from the crop, and your brothers go empty away.

Ye may kill for yourselves, and your mates, and your cubs as they need, and ye can;
But kill not for pleasure of killing, and seven times never kill Man!

If ye plunder his Kill from a weaker, devour not all in thy pride;
Pack-Right is the right of the meanest; so leave him the head and the hide.

The Kill of the Pack is the meat of the Pack. Ye must eat where it lies;
And no one may carry away of that meat to his lair, or he dies.

The Kill of the Wolf is the meat of the Wolf. He may do what he will;
But, till he has given permission, the Pack may not eat of that Kill.

Cub-Right is the right of the Yearling. From all of his Pack he may claim
Full-gorge when the killer has eaten; and none may refuse him the same.

Lair-Right is the right of the Mother. From all of her year she may claim
One haunch of each kill for her litter, and none may deny her the same.

Cave-Right is the right of the Father — to hunt by himself for his own:
He is freed of all calls to the Pack; he is judged by the Council alone.

Because of his age and his cunning, because of his gripe and his paw,
In all that the Law leaveth open, the word of your Head Wolf is Law.

Now these are the Laws of the Jungle, and many and mighty are they;
But the head and the hoof of the Law and the haunch and the hump is — Obey![122]

[122] R. Kipling, The Jungle Book (1894), The Law of the Jungle.

3 Social Contract Theory on State Sovereignty

NOW this is the Law of the Jungle — as old and as true as the sky; And the Wolf that shall keep it may prosper, but the Wolf that shall break it must die.[123]

3.1 Introduction

As explained in Chapter 2, because of the trends in the digital universe of acceleration, miniaturization and dematerialization, the constituting dimensions of the digital universe are expanding into and merging with, the physical universe. Resultantly, cyberspace is everywhere, accessible by everyone and connected to everything. With this increased presence of cyberspace comes the question whether this new space can or should fall within the realm of State sovereignty. In other words, should cyberspace be another sovereign space, akin or analogous to other spaces which already fall under State sovereignty, such as terrestrial territory, internal- and territorial waters and water- and territorial airspace?[124] Or, alternatively, should cyberspace perhaps be a space which remains the Common Heritage of Mankind, akin or analogous to other spaces which are already the Common Heritage of Mankind, such as the high seas[125] and outer space?[126]

Cyber libertarians and anarchists have argued since the 90s that cyberspace is a naturally free space and that it therefore also naturally falls beyond the sovereignty of States.[127] Cyber libertarians hence argue that cyberspace should be regarded as a space which is the Common Heritage of Mankind.[128] This position was captured and expressed famously (and quite beautifully) by poet and cofounder of the Electronic Frontier Foundation, John Barlow, in his internet manifesto at the World Economic Forum in 1996.[129] The historical setting of this manifesto is important in order to provide the context in which it was written. At the time, Barlow had been attending the elite World Economic Forum in Davos, Switzerland for the past four days, where world leaders in government, business and philanthropy had been setting out

[123] R. Kipling, The Jungle Book (1894), The Law of the Jungle.
[124] *See supra* note 12.
[125] *See supra* note 12.
[126] *See supra* note 17.
[127] *See e.g.*, J. Barlow, A Declaration of the Independence of Cyberspace, World Economic Forum, Davos, Switzerland, February 8, 1996, available at: https://www.eff.org/cyberspace-independence (accessed on 31st July, 2017).
[128] *Id.*
[129] *See* Barlow, A Declaration of the Independence of Cyberspace.

their positions on cyberspace and their goals and strategies on how to control it. Simultaneously, on the same day, President Bill Clinton signed the Communications Decency Act into law, which empowered the Federal Communications Commission (FCC) to ban the transmission of obscene material on the Internet just as it did on radio and network television. Barlow, a cyber libertarian, must have felt like Mankind was about to lose cyberspace, a space he believed deeply should be the property of Mankind as a collective and not the property of individual States. His manifesto announced to the "[g]overnments of the industrial world", those "weary giants of flesh and steel" that they have no place in cyberspace and that they should stay away from the "tyrannies [they] seek to impose on us".[130] After all, "Governments derive their just powers from the consent of the governed" and, Barlow continued, "[they] have neither solicited nor received ours.".[131] Rather, cyberspace, those captured and cultivated parts of the digital universe where Mankind has created order and civilization out of the vast chaos and wilderness, according to Barlow and others, will either be self-governed by the good will of the people or, alternatively, they are "naturally independent" because States do not possess "any methods of enforcement we have true reason to fear".[132]

Barlow's claims are powerful and his arguments need to be addressed. There are two main arguments; one of right and one of might. If Mankind has never, implicitly or explicitly, surrendered control over cyberspace to States and if Mankind was the original rightful owner, then by what *right* then can States claim control over it? And, even if Mankind has had the original rightful ownership over cyberspace and has since chosen to surrender it, by what *might* can the non-physical domain of cyberspace even be effectively controlled by States? What method of enforcement does one use in a world which is digital?

Any legal theory which proclaims that (parts of) cyberspace ought to fall within the realm of State sovereignty, needs to provide convincing arguments that (parts of) this new space should in fact fall within the realm of state sovereignty and will have to do so pursuant to the legal theory on State sovereignty.

---

[130] *Id.*
[131] *Id.*
[132] Barlow, A Declaration of the Independence of Cyberspace: "Where there are real conflicts, where there are wrongs, we will identify them and address them by our means. […] It is an act of nature and it grows itself through our collective actions. […] Our identities have no bodies, so, *unlike you, we cannot obtain order by physical coercion*. We believe that from ethics, enlightened self-interest, and the commonweal, our governance will emerge. Our identities may be distributed across many of your jurisdictions. The only law that all our constituent cultures would generally recognize is the Golden Rule. We hope we will be able to build our particular solutions on that basis.". (emphasis added); *see also* Section 2.2. Barlow uses cyberspace where I would use 'digital universe'.

In this dissertation, I will argue that cyberspace is indeed to some extent an inherently free space, as argued by Barlow and others like him. Contrary to them however, I argue that this freedom is not unlimited and I argue this position precisely because cyberspace concerns those captured and cultivated parts of the digital universe where Mankind has created order and civilization out of the vast chaos and wilderness. To use Barlow's phrasing; I posit that cyberspace is naturally *dependent* upon State sovereignty – at least partially.[133] Thereto, I will argue that (certain) parts of cyberspace can, do and will fall in the realm of State sovereignty. In other words, I will argue that there is both a right of States to control parts of cyberspace and a might to do so. More specifically, I will point at two types of activities in cyberspace which clearly do fall within the realm of State sovereignty - namely the protection against large-scale theft of intellectual property and the protection against durable disruption of critical infrastructures. In Chapter 5, I will deal in depth with large-scale theft of intellectual property and argue that this is as severe as territorial aggrandizement. In Chapter 6, I will deal in depth with durable disruption of critical infrastructures and argue that this is as severe as a territorial blockade. These are the questions of right. In Chapter 4, I will deal with the question of might as I discuss how to establish effective control over the domain of cyberspace.

In this chapter specifically, I will build the theory that will be used in Chapters 4-6 to argue that the protection against large-scale theft of intellectual property and durable disruption of critical infrastructures in cyberspace does, in fact, fall within the realm of State sovereignty. Thereto, I will argue that the applicability of the principle of State sovereignty over any space – whether it is land, air, water or cyber - is conditional upon two principles; 1. use of force can be exercised there to inhibit the self-determination of the individuals present there (this is the part which concerns the question of *right*), and 2. States are able to exercise effective control over these spaces to prevent this use of force (this is the part which concerns the question of *might*). The theoretical basis for these two principles will be laid in this current chapter. They will be applied practically to the domain of cyberspace in Chapters 4-6. In Chapter 4, I will deal in depth with principle 2 and the criteria of effective control. In Chapters 5 and 6, I will deal with principle 1 and the criteria of the use of force.

In order to set out the theoretical framework for the applicability of State sovereignty over a certain space, I will take an historical approach and build the theory from the ground up. Thereto, Section 3.2 will first deal with the laws of *nature*. It will explain that in the state of

[133] *See supra* note 132.

nature, each life form – which includes us as *homo sapiens* -, acts in accordance with an inherent drive to self-determination and will therefore act in self-preservation in any way deemed necessary for the twin goals of survival and reproduction. Among the indispensable instruments for the pursuit of these goals, I will argue, is the use of force. Subsequently, Section 3.3 will deal with the laws of *men*. It will take the findings of 3.2 and extrapolate them to their logical, natural conclusion. It will explain why acting in self-interest logically and naturally points towards the agreement among men to recognize each other's right to self-determination so that they may each enjoy better lives. In this section, I will also explain that this right logically and naturally entails a prohibition on the use of force aimed against the life, liberty and property of other participants to the agreement. Following this, Section 3.4 will deal with the laws of *States.* It will explain why the legitimacy of the State is originated upon the protection of the life, liberty and property of its citizens and their collective expression as a people - both within the State between individual citizens and beyond the State from external aggression. It will explain that this legitimacy upon which State sovereignty rests, is conditional upon the degree to which the State can exercise effective control over the protection of these interests within given spaces – such as territorial-, water-, air- and cyberspace. Finally, Section 3.5 will deal with the laws of the *international order*. In this section, I will move the discussion on the prohibition on the use of force to the international level and explain, pursuant to the domestic analogy, why the protection of sovereign existence, political independence and territorial integrity are the collective forms of the protection of life, liberty and property in the state of nature which exists not between individuals, but between States. This section will also explain why the legitimacy of the international legal order is similarly conditional upon the effectiveness of the international legal order to protect States from the use of force against them, especially when it is directed against their sovereign existence, political independence and territorial integrity.

In sum, this present chapter will deal with the *theory* of State sovereignty over spaces in general and argue that it rests upon the effective control within certain spaces to protect the lives, liberty and property of the individuals living there, as well as their collective expressions as sovereign existence, political independence and territorial integrity. In the following chapters, this theory will be applied in *practice* to the domain of cyberspace specifically. Chapter 4, will deal with the effective control part of the equation and apply it to the domain of cyberspace. Chapters 5 and 6, will elaborate on this and deal with the areas where States can exercise use of force against the life, liberty and property of people through cyberspace. Chapter 5 will argue that large-scale intellectual property theft constitutes a use of force which States

need to (be able to) protect its citizens against. Chapter 6 will argue the same for durable disruption of critical infrastructures.

3.2 On the Laws of Nature

In nature, every life form acts according to its perceived self-interest in order to survive and to reproduce. Doing so is the *conditio sine qua non* for its continued existence and reproductive success in an environment where there is competition for scarce resources - such as food and reproductive opportunities. Pursuant to the law of the jungle and evolutionary biology, the zebra competes with other zebras for greener grazing pastures, the lion hunts the zebra for food in order to sustain himself and when this almighty king of the jungle comes home, he has to fight off other lions for the possibility to mate.

In nature, there are many strategies for competing successfully. Some life forms get their energy directly from the sun in the sky (*i.e.* photosynthesis) or from hydrothermal vents at the bottom of the ocean (*i.e.* chemosynthesis). Other life forms get their energy by consuming these former life forms (*i.e.* herbivores) and even other life forms consume this latter category (*i.e.* carnivores). In this competition for scarce resources, life forms can compete between and across species and they can do so through conquest and through cooperation. Although cooperation - such as the zebra moving in herds to decrease the chances of being killed and the lion moving in prides in order to increase the chances of a successful hunt - seems more social, noble and less conflictuous than conquest, in fact, this strategy of cooperation, when properly understood, is, just like conquest, simply another strategy by which the ability of the individual to compete successfully against others and against other groups in a world of scarce resources, is increased pursuant to self-interest.

Homo sapiens is no exception to the laws of nature. Man acts according to his perceived self-interest in order to survive and to reproduce. Doing so is the *conditio sine qua non* for his continued existence and reproductive success in an environment where there is competition for scarce resources - such as food and reproductive opportunities. Initially, man did not make much use of the strategy of cooperation - kinship and kindness were instead reserved for next of kin and kind only.[134] Instead, the preferred tactics and strategies were based on conquest.[135]

[134] *See generally* S. Pinker, The Better Angels of Our Nature – Why Violence has Declined (2012) (hereinafter: "The Better Angels of Our Nature"), Chapters 1-2 (2012). Bedouin proverb: "I against my brother, I and my brother against our cousin, I, my brother and our cousin against the neighbors, all of us against the foreigner.".
[135] *See generally* Pinker, The Better Angels of Our Nature, Chapters 1-2 (2012).

Whenever an individual or a band of people perceived that it could best further its interests through the use of force, by killing, raping and stealing from individuals within the group or from another band of people, then inhibitions from doing so were merely of a pragmatic, tactical or strategic nature - and *vice versa*.[136] *Homo homini lupus est.*

In this competition within and between these individuals and bands of people, the individual bears the ultimate responsibility for maintaining the ability to the self-determination of his own tactics and strategies. Because of this original situation where (attempts at) conquest by others was such a common occurrence, the use of force is an indispensable instrument for the individual to do so. Given this fact and because acting in self-preservation when one's ability to the self-determination of his own tactics and strategies is threatened, is so closely connected to (human) nature and instinct, it should come as no surprise that throughout the history of legal and political philosophy, various authorities have attempted to describe the right to act in self-preservation through self-defense against aggression in superlative degrees of being supreme and, above all as being 'natural'.[137] This connection of one's right to self-defense to human nature is said to be caused by ones 'inborn', 'innate' or 'inherent' desire to protect those interests which are vital to one's self-preservation.[138] Darwinian evolution, that universal law of biological nature, has selected for those individuals with the burning desire to fight for their survival when their lives are threatened and selected against those who didn't, wouldn't or couldn't. The result of this is that *homo sapiens* – just like the rest of the animal kingdom - naturally acts in self-preservation and will use force whenever necessary.

Because of this, in this original situation, the individual may and will do so by any and all means, *i.e.*, he may use force in self-defence pre-emptively, preventively, punitively or in any manner deemed necessary for self-preservation.[139] As in this original situation there are

---

[136] *Id.*

[137] *See especially* T. Hobbes, Leviathan, Chapter XIV (1651): "The RIGHT OF NATURE, which Writers commonly call *Jus Naturale, is the Liberty each man hath, to use his own power, as he will himselfe, for the preservation of his own Nature*; that is to say, of his own Life; and consequently, of doing any thing, which in his own Judgement, and Reason, hee shall conceive to be the aptest means thereunto.". (emphasis added)

[138] *Id.*

[139] *See* Hobbes, *Leviathan*, Chapter XIV: "The RIGHT OF NATURE, which Writers commonly call Jus Naturale, is the Liberty each man hath, to use his own power, as he will himselfe, for the preservation of his own Nature; that is to say, of his own Life; and consequently, *of doing any thing, which in his own Judgement, and Reason, hee shall conceive to be the aptest means thereunto.*" (emphasis added); *see also* J. Locke, *Two Treatises of Government: In the Former, The False Principles, and Foundation of Sir Robert Filmer, and His Followers, Are Detected and Overthrown. The Latter Is an Essay Concerning The True Original, Extent, and End of Civil Government, Second Treatise* (1689) (hereinafter: "Second Treatise of Government", Chapter II, sect. 8: "in the state of nature, one man comes by a power over another; but yet no absolute or arbitrary power, to use a criminal, when he has got him in his hands, according to the passionate heats, or boundless extravagancy of his own will; but *only to retribute to him, so far as calm reason and conscience dictate, what is proportionate to his*

none other than oneself to protect one's interests, none can be there to inhibit one's protection of these interests either.[140] Whereas modern legal systems would prohibit most of these types of self-defence, few would call for similar prohibitions in this original situation.[141] Instead, beasts bear no burdens of boundaries in this a-moral state of nature and man is allowed, pursuant to his natural rights to act in self-preservation, to do whatever is deemed necessary.[142] Indeed, in this original situation where contact with others was mostly to be feared, one often *has* to act pre-emptively, preventively and/or punitively, because such actions are often necessary for the effective deterrence of both the immediate and potential future aggression.[143] There is great

---

transgression, which is so much as may serve for reparation and restraint: for these two are the only reasons, why one man may lawfully do harm to another, which is that we call punishment.". (emphasis added), Chapter II sect. 12: "By the same reason may a man in the state of nature punish the lesser breaches of that law. It will perhaps be demanded, with death? I answer, *each transgression may be punished to that degree, and with so much severity, as will suffice to make it an ill bargain to the offender, give him cause to repent, and terrify others from doing the like*." (emphasis added) Locke continues in section 12 by inserting a disclaimer that it is "besides [his] present purpose, to enter here into the particulars of the law of nature or the measure of punishment". Although this mentioning of proportionality seems to indicate a somewhat measured or limited response, the justification for acting against transgression are reparation and restraint. The latter of these justifications, would, when properly applied to a state of nature situation, entail a measure of force which would be hard to classify as 'proportional' under modern definitions thereof, instead being pre-emptively, preventively, punitively or in any manner deemed necessary. Given the lack of information about enemy behavior, the default modus for behavior would be to assume a policy of overwhelming aggression. Only reasons of a pragmatic nature of self-interest would dictate otherwise sometimes, not natural law.

[140] *See* Hobbes, *Leviathan*, Chapter XIII: "To this warre of every man against every man, this also is consequent; that *nothing can be Unjust. The notions of Right and Wrong, Justice and Injustice have there no place. Where there is no common Power, there is no Law: where no Law, no Injustice*. Force, and Fraud, are in warre the two Cardinall vertues. Justice, and Injustice are none of the Faculties neither of the Body, nor Mind. If they were, they might be in a man that were alone in the world, as well as his Senses, and Passions. *They are Qualities, that relate to men in Society, not in Solitude. It is consequent also to the same condition, that there be no Propriety, no Dominion, no Mine and Thine distinct; but onely that to be every mans that he can get; and for so long, as he can keep it.*". (emphasis added); *see also* Locke, *Second Treatise of Government*, Chapter II, sect. 6: "But though this be a state of liberty, yet it is not a state of licence: […] The state of nature has a law of nature to govern it, which obliges every one: and *reason, which is that law, teaches all mankind, who will but consult it, that being all equal and independent, no one ought to harm another in his life, health, liberty, or possessions*:". (emphasis added). Contrary to Hobbes, Locke's legal theory is predicated and build on the notion that a universal law of nature exists - which is reason - which governs even 'lawless' situations. Although it seems entirely possible for all men to understand that other men may or will have the same vital interests as he does, the categorization of such a realization as law seems like confounded wishful thinking which reflects a poor understanding of the state of nature – which is based on might, not right.

[141] *Id.*

[142] *Id.*

[143] *See* Locke, *Second Treatise of Government*, Chapter II, sect. 11: "[…] the damnified person has this power of appropriating to himself the goods or service of the offender, by right of self-preservation, as every man has a power to punish the crime, *to prevent its being committed again*, by the right he has of preserving all mankind, and doing all reasonable things he can in order to that end: and thus it is, that *every man, in the state of nature, has a power to kill a murderer, both to deter others from doing the like injury*, […] by the unjust violence and slaughter he hath committed upon one, declared war against all mankind, and therefore may be destroyed as a lion or a tyger, one of those wild savage beasts, with whom men can have no society nor security: and upon this is grounded that great law of nature, Whoso sheddeth man's blood, by man shall his blood be shed.". (emphasis added) Although Locke's argumentation is predicated and build upon the notion that a universal natural law is transgressed through which the transgressors has placed himself not in the society of Mankind, but in the Kingdom of nature, even without this argumentation Locke emphasizes the need for effective deterrence of transgressions against the vital interests of men.

tactical and strategic benefit for the individual in striking first, in striking hard and in striking often.

Philosophers have theorized what game-theorists have modeled and what anthropologists, primatologists and archeologists have discovered to be true in practice, namely that the result of the incentive to strike first, hard and often which exists in the state of nature is a *bellum omnium contra omnes*, a war of all against all.[144] In the original situation where each man acts pre-emptively, preventively and punitively in self-preservation, waging war is in fact the logical, natural option for all and it happens everywhere, all the time.[145] War is a constant factor of life.[146] Resultantly, as famously and brilliantly stated by Hobbes, there is "continual fear, and danger of violent death; and the life of man, solitary, poor, nasty, brutish, and short.".[147]

However, although this original situation of war of all against all is the natural state and although it is the result of logical choices pursuant to self-interest on the micro-level by each individual man, it is not the optimal utilitarian result pursuant to the collective self-interest on the macro-level for Mankind.[148] As will be explained in more detail in the next section, through

---

[144] *Cf*. Hobbes, *Leviathan*, Chapter XIII "From this equality of ability, ariseth equality of hope in the attaining of our Ends. And therefore if any two men desire the same thing, which neverthelesse they cannot both enjoy, they become enemies; and *in the way to their End*, (which is principally their owne conservation, and sometimes their delectation only,) *endeavour to destroy, or subdue one another*. […] There Is Alwayes Warre Of Every One Against Every One Hereby it is manifest, that *during the time men live without a common Power to keep them all in awe, they are in that condition which is called Warre; and such a warre, as is of every man, against every man*.". (emphasis added); *see also generally* Pinker, The Better Angels of Our Nature, Chapters 1-2 (2012). Archaeologists and anthropologists have, respectively, discovered and observed that peoples living in a state of nature, both past and present, live in a situation in which war is far more prevalent than in environments where the State has monopolized violence. Despite modern methods of killing, the chance of dying by another person's hands is much greater in the state of nature; *see e.g. generally* J. Goodall, *Through a Window: My Thirty Years with the Chimpanzees of Gombe* (2010). Goodall is a famous primatologist who studied *Pan troglodytes* (chimpanzee), our evolutionary closest living relative. Goodall observed that chimpanzees regularly engage in genocidal wars with other groups of chimps.

[145] *Id.*

[146] *Id.*

[147] *See* Hobbes, *Leviathan*, Chapter XIII: "*Whatsoever therefore is consequent to a time of Warre, where every man is Enemy to every man*; the same is consequent to the time, wherein men live without other security, than what their own strength, and their own invention shall furnish them withall. […] and which is worst of all, continuall feare, and danger of violent death; *And the life of man, solitary, poore, nasty, brutish, and short*.". (emphasis added)

[148] *See* Hobbes, *Leviathan*, Chapter XIII: "And from hence it comes to passe, that where an Invader hath no more to feare, than another mans single power*; if one plant, sow, build, or possesse a convenient Seat, others may probably be expected to come prepared with forces united, to dispossesse, and deprive him, not only of the fruit of his labour, but also of his life, or liberty*. And the Invader again is in the like danger of another.". […]In such condition, there is no place for Industry; because the fruit thereof is uncertain; and consequently no Culture of the Earth; no Navigation, nor use of the commodities that may be imported by Sea; no commodious Building; no Instruments of moving, and removing such things as require much force; no Knowledge of the face of the Earth; no account of Time; no Arts; no Letters; no Society […].". (emphasis added)

cooperation, the interests of the whole can be served to a greater extent than the sum of its parts can be in the original situation of constant conquest.

Before we come to explaining the mechanisms underlying this stated conclusion, it is important to explore first whether it is in the interest of *all* men to cooperate. After all, if there are exceptions by which some men can pursue their self-interest better through conquest in this war of all against all, then cooperation is not in their self-interest and they will hence not wish to cooperate with others. Fortunately, these exceptions do not seem to exist in any way which would warrant hesitance against taking cooperation as the goal to pursue. Since the nature of Mankind is such that all men are essentially 'equal in body and mind', no man can successfully conquer all consistently.[149] Although one man may be significantly or even overwhelmingly stronger than another or even than many - both in faculties of mind and body - during a specific time-frame and although this physical or mental superiority might create a want in a man to claim and exercise a right of might when his competitive advantage is such, there is always the eventual necessity of sleep, the fading of one's physical and mental faculties with age and the danger of groups ganging up on one when political allegiances change.[150] Conquest therefore is a long-term successful strategy for no man.

Hence, since no man can consistently pursue his self-interest best through conquest, in order to increase one's chances of competing successfully, acting in self-preservation naturally and logically entails increasing cooperation with others along certain agreements on common interests. The reason why cooperation can be the mode of interaction which has the most positive cost/benefit outcome for the collective, is because, as pointed out by Dawkins, in nature there are many so-called non-zero sum games.[151] Whereas in *zero*-sum games the gains of one of the players necessarily must come at the expense of the other player(s), and hence conquest is the optimal tactical and strategical choice in these games, in *non-zero*-sum games, the gains

[149] *See* Hobbes, *Leviathan*, Chapter XIII: "*Nature hath made men so equall, in the faculties of body, and mind; as that though there bee found one man sometimes manifestly stronger in body, or of quicker mind then another; yet when all is reckoned together, the difference between man, and man, is not so considerable,* as that one man can thereupon claim to himselfe any benefit, to which another may not pretend, as well as he.". (emphasis added); *see* Locke, *Second Treatise of Government*, Chapter II, sect. 4: "*A state also of equality*, wherein all the power and jurisdiction is reciprocal, no one having more than another; there being nothing more evident, than that creatures of the same species and rank, *promiscuously born to all the same advantages of nature, and the use of the same faculties, should also be equal one amongst another* without subordination or subjection, unless the lord and master of them all should, by any manifest declaration of his will, set one above another, and confer on him, by an evident and clear appointment, an undoubted right to dominion and sovereignty.". (emphasis added)

[150] *See* Hobbes, *Leviathan*, Chapter XIII: "For as to the strength of body, *the weakest has strength enough to kill the strongest, either by secret machination, or by confederacy with others, that are in the same danger with himselfe*.". (emphasis added)

[151] *See* R. Dawkins, The Selfish Gene, at 202-240.

of each of the players can come not necessarily only at the expense of the other player(s), but also at the expense of the 'house' (which is a metaphor for an optimal result), thus warranting cooperation to 'beat the house'.[152] In other words, in non-zero-sum games, as opposed to zero-sum games, the players have the possibility to play the game in such a way that they do not compete against each other for a larger part of the same pie, but rather, that they can instead cooperate to compete together against the house for a larger pie than had previously been accessible.[153] By sharing the spoils which come at the expense of the house, the interests of both players can hence be better served and resultantly, they can compete better than those who do not cooperate.[154] For example, two small groups of hunter/gatherers wandering the same forest can agree, implicitly or explicitly, to no longer kill, rape and steal from the other group. Although this agreement does not change anything about the carrying capacity of the forest – such as the amount of animals living or plants growing there -, it does greatly reduce the amount of time and energy both groups have to spend in preparation of, waging of and recovering from war against the other group. Men can hunt animals without the fear of coming home with their kills stolen, women can gather fruits, nuts and vegetables without the fear of being raped or kidnapped and none have to spend the same amount of time in the preparation for, waging of and recovering from war against the other. All this recovery from wasted hunts and loss of life, health and productivity, as well as those costly setbacks of insurance policies through preparations for fear of such setbacks, can be diminished, thereby negating the great expenses in time and energy which were previously necessary for continued secured survival.

Correspondingly, through cooperation, there can be a great increase in the amounts of time and energy both groups can spend on finding food and on reproducing. In other words, through cooperation and non-conquest, both groups can serve their own respective interests better than they could previously and they can therefore now also compete more successfully against other groups which do not have such arrangements with their neighboring groups. The resources of time and energy can be spend much more productively through cooperation. The pie grows.

In sum, the laws of nature are such that *homo sapiens* – like all other life forms -has a natural instinct and right to use force to act in self-preservation and that he may do so preventively, pre-emptively and punitively. However, given the war of all against all that this

[152] *Id.*
[153] *Id.*
[154] *Id.*

original situation naturally creates, this situation is not the optimal result for the pursuit of one's self-interest. Moreover, this is true for everyone. A strategy of conquest in this original situation is the optimal result for no one. Rather, self-determination logically points to attempting to cooperate so that people can compete not against each other for a larger share of the same pie, but against the house for a share of a new, larger pie. The condition for achieving this is however that they can achieve an agreement on which common interests they can cooperate on and an approach on how to achieve these interests. The next sections will deal with these interests and the ways to achieve them. Generally speaking Section 3.3 will deal with which common interests are naturally, logically arrived at and Section 3.4 will deal with which tactics and strategies are naturally and logically employed in this pursuit, namely the appointment of a neutral arbiter of disputes in the shape of a State.

3.3 On the Laws of Men

From this original situation, these common interests can be rationally arrived at and distilled into the acceptance of the single agreement among participants of the mutual recognition of one another's right to self-determination, *i.e.*, the recognition of the right of each individual in the agreement to pursue one's own self-interest according to one's own tactics and strategies without being limited in this pursuit by other participants to the agreement through the use of force.[155] Such an agreement frees one from the burden of having to spend much of his time and energy in preparing for, conducting off and recovering from war against aggression from the other participants to the agreement using force against him - as such is no longer necessary *vis-à-vis* the other participants to the agreement (at least, not so long as the agreement is kept or so long as it is perceived that it will stay kept). Slowly but surely, these agreements not to use force let participants compete successfully against other groups which did not have such agreements.

Consequently and eventually, this agreement and agreements like it would free up the time, energy and security which would end up laying the basis for modern civilization. Prior to the laws of men, there could be "no place for Industry; because the fruit thereof is uncertain; and consequently no Culture of the Earth; no Navigation, nor use of the commodities that may

[155] *See* Hobbes, *Leviathan*, Chapter XIV: "By liberty is understood, according to the proper signification of the word, the absence of external impediments; which impediments may oft take away part of a man's power to do what he would, but cannot hinder him from using the power left him according as his judgement and reason shall dictate to him.".

be imported by Sea; no commodious Building; no Instruments of moving, and removing such things as require much force; no Knowledge of the face of the Earth; no account of Time; no Arts; no Letters; no Society".[156] In other words, without the security provided by the laws of men, no one would find it a risk worthy tactic or strategy to invest the time, energy and resources necessary to produce advanced products – such as 'Culture of the Earth' -, which could simply be stolen or destroyed after production.[157] Similarly, as will be discussed in extensive detail in Chapter 5, without the laws of men, there would not be the trade and specialization of profession which is necessary to result in advanced services either – such as research into the 'Knowledge of the face of the Earth'.[158] Without the agreement on the mutual right to self-determination, life would be poor indeed.

This agreement of the mutual recognition of one another's right to self-determination, *i.e.*, the recognition of the right of each individual in the agreement to pursue one's own self-interest according to one's own tactics and strategies without being limited in this pursuit by other participants to the agreement through the use of force, entails the prohibition by participants to the agreement of any actions which could force other participants to the agreement to act in a manner not of their own volition.[159] It requires an 'absence of external impediments'. A variety of philosophers and authors have enumerated different interests which would need to be respected to enable the right to self-determination to be exercised.

A comparison of these and other philosophers leads to the *grosso modo* classification of *life*, *liberty* and *property* as the vital interests which need to be protected by the agreement.[160] This classification, I will demonstrate later in this section, is no accident, but rather, as I will argue, reflects law derived from (human) nature. Thus, the agreement of recognition of one

---

[156] *See* Hobbes, *Leviathan*, Chapter XIII.
[157] *Id.*
[158] *Id.*
[159] *Id.*
[160] *Cf.* Locke, *Second Treatise of Government*, Chapter II, Sect. 6: "*Every one, as he is bound to preserve himself*, and not to quit his station wilfully, so by the like reason, when his own preservation comes not in competition, ought he, as much as he can, to preserve the rest of mankind, and may not, unless it be to do justice on an offender, take away, or *impair the life, or what tends to the preservation of the life, the liberty, health, limb, or goods* of another.", Chapter VII, sect. 87: " Man being born, as has been proved, with a title to perfect freedom, and an uncontrouled enjoyment of all the rights and privileges of the law of nature, equally with any other man, or number of men in the world, *hath by nature a power, not only to preserve his property, that is, his life, liberty and estate*, against the injuries and attempts of other men; but to judge of, and punish the breaches of that law in others, as he is persuaded the offence deserves, even with death itself, in crimes where the heinousness of the fact, in his opinion, requires it. (emphasis added); J. Rousseau, On the Inequality among Mankind (1754), part II: "[…] For what reason, in fact, did they take to themselves superiors, if it was not in order that they might be defended from oppression, and have *protection for their lives, liberties and properties*, which are, so to speak, the constituent elements of their being?". (emphasis added)

another's right to self-determination entails the agreement of recognition that each individual has a mutual and reciprocal vital interest to the protection of his life, liberty and property and that no force may be used by those entering into the agreement which threaten or attack these interests by the other participants to the agreement.

For the purposes of this dissertation, these interests need to be defined. As announced in the introduction to this chapter, I will argue that (parts of) cyberspace must necessarily fall within the realm of State sovereignty as they constitute a minimum threshold for any society to meet in order for it to be able to survive. Given that my justification for this claim will be built on the interests I am about to define, I will try to define these interests rather narrowly. An overly expansive definition would provide shaky foundations for the theory I am building on top of it. I will therefore try to err on the side of caution. Others may have more expansive or more restrictive definitions of these interests, but this is how I define them for the purposes of this dissertation.

The interest to 'life' should be seen as one's very existence and one's physical integrity, *i.e.*, one's life and limb, or one's physical 'person'.[161] This right is the constituting biological prerequisite for one's self-preservation. Any use of force against the whole or part of life or the body, through murder, assault, torture or other use of force, is a direct attack on one's self-preservation and an inhibition of one's right to self-determination. The interest of an individual to his 'life' should naturally be deemed to enjoy the status of being the supreme and ultimate interest among the three.

The interest to 'liberty' should be seen as one's interest to pursue one's own self-interest pursuant to one's own choosing, tactics and strategies.[162] This right can be described as the psychological prerequisite for life in the sense that the biological prerequisite to life is of little value when one is imprisoned.[163] Life, in essence, is about being free, about self-determination. Any agreement which guarantees life at too great an expense to liberty will naturally be rejected

[161] *See supra* note 160; *see also* Locke, *Second Treatise of Government*, Chapter XIX, sect. 233: "for it is natural for us to defend life and limb"; *see also* Rousseau, On the Inequality among Mankind, part II: "Man's first feeling was that of his own existence, and *his first care that of selfpreservation*." (emphasis added)
[162] *See supra* note 160; *see also* Hobbes, *Leviathan*, Chapter XIV: "By LIBERTY, is understood, according to the proper signification of the word, the absence of externall Impediments: which Impediments, may oft take away part of a mans power to do what hee would; but cannot hinder him from using the power left him, according as his judgement, and reason shall dictate to him.".
[163] *Id. See also* Rousseau, On the Inequality among Mankind, part II: For what reason, in fact, did they take to themselves superiors, if it was not in order that they might be defended from oppression, and have protection for their lives, liberties and properties, which are, so to speak, *the constituent elements of their being*?". (emphasis added)

and have no participants. Hence, any use of force against the freedom of an individual to freely determine one's tactics and strategies in the pursuit of one's goals, through imprisonment, slavery, forced labour or other threats of force, is a direct attack on self-determination. The interest of an individual to his 'liberty' should be deemed as an indispensable interest which gives substance to the interest to life. Without liberty, there can be no life worth living.

The interest to 'property' finally, describes one's material goods and possessions, the fruits of one's labor, the means of one's livelihood.[164] Although it is tempting for the present writer for alliteration purposes to choose the term 'livelihood' as the third protected vital interest, the term does not accurately reflect the protected interest. Livelihood refers to the means through which one secures the basic necessities to sustain oneself - such as the immediate resources of air, water, food, and clothing and possibly also the less immediate resources of safety and security, such as shelter. Any property freely acquired beyond these basic necessities does not fall under the category of livelihood. Products and services acquired for purposes of belonging, esteem, self-actualization or simple want of luxury would hence not fall within the term livelihood. Although it is clear that livelihood would be a suitable term to describe the interests one would need to protect for immediate and semi-immediate physiological security, the term does not encompass the full scale of property against which use of force could be exercised to inhibit one's right to self-determination. Although a use or threat to use force against one's house or place of business would entail a stronger inhibition on one's right to self-determination than would a use or threat to use force against one's second house, nonetheless, all would inhibit one's right to self-determination. After all, one can imagine that someone has spent years of his life building such a house. When force is used (or threatened) against this property, it is, in essence, (a threat of) force against these years of one's life. When the house is destroyed, this person is retroactively no longer able to freely pursue his own self-interest according to his own tactics and strategies during that time. Although the protection of property can be placed lowest among the three interests, it must be asserted that the protection of one's material goods constitutes a physical prerequisite for one's life and liberty when it comes to the protection of basic property for physiological and safety and security needs. We are after all not animals whose means of attaining food or having shelter are attached to our physical bodies in the form of, respectively, claws or fur. Rather, these means have been externalized and have taken the form of property. (Chapter 6 will deal with this in-depth.) Additionally, any use of

[164] *See supra* note 160; *see also infra* Sections 5.25.4. Chapter 5 in general and Sections 5.25.4 in particular are dedicated to describing property as a vital interest.

force – such as theft or otherwise barring access to freely determine what to do with one's property – against the property which doesn't serve a direct physiological need, but merely a psychological want, can also force an individual to act in a manner not of his own volition and should therefore also fall within the agreement to the mutual right of self-determination.

As we take a leap forward in time and look at established States and other legal systems, we find that beyond the protection of these interests of life, liberty and property in philosophy and theory by the most authoritative political philosophers, as we have just discussed, we also find these same interests protected as rights in law and practice in the most authoritative legal documents.

On the global level, the 1948 United Nations Declaration of Human Rights (hereinafter: "UN Declaration of Human Rights") – which is arguably one of the most authoritative and formative documents of our modern global civilization - after having dealt with the articles on equality[165] and non-discrimination,[166] starts in article 3 with the articles on the protection of life and liberty by declaring that "[e]veryone has the right to *life, liberty* and *security of person.*".[167] In other words, the UN Declaration of Human Rights declares that the first substantive human right, is the protection of the right to life and liberty, thus corresponding to what we have seen are the natural and logical supreme and ultimate interests any rational person serving his self-interest would want to protect. After dealing with several additional articles on how to substantively protect these rights to life and liberty – such as the protection from slavery,[168] torture,[169] having one's liberty taken away through arbitrary arrest or through a lack of due legal process,[170] restrictions of movement[171] and from being forced into a marriage not of one's own choosing[172] -, it continues in article 17 with the protection of property by declaring that "(1) Everyone has the right to own *property* alone as well as in association with others. (2) No one shall be arbitrarily deprived of his *property*.".[173] (emphasis added) In other words, the primary rights which this foundational document of the international legal order seeks to protect are the rights to life, liberty and property, thus corresponding to the most supreme and ultimate interests any rational person serving his self-interest would want to protect. Throughout the UN

[165] Article 1 United Nations Declaration of Human Rights.
[166] Article 2 United Nations Declaration of Human Rights.
[167] Article 3 United Nations Declaration of Human Rights.
[168] Article 4 United Nations Declaration of Human Rights.
[169] Article 5 United Nations Declaration of Human Rights.
[170] Article 6-11, 14-15 United Nations Declaration of Human Rights.
[171] Article 13 United Nations Declaration of Human Rights.
[172] Article 16 United Nations Declaration of Human Rights.
[173] Article 17 United Nations Declaration of Human Rights.

framework, codifications of these same rights can also be found. The 1966 International Covenant on Civil and Political Rights (hereinafter: "ICCPR"), one of the most important universal human rights documents, starts in article 6 with the rights to physical integrity by stating that the parties to the covenant agree that "[e]very human being has the *inherent right to life.* This right shall be protected by law. No one shall be arbitrarily deprived of his *life*.".[174] (emphasis added) In article 9 the covenant continues with the liberty and the security of person by stating that "[e]veryone has the *right to liberty* and *security of person*. No one shall be subjected to arbitrary arrest or detention. No one shall be deprived of his *liberty* except on such grounds and in accordance with such procedure as are established by law.".[175] (emphasis added)

On the European level, codifications of these same rights and the protection against their encroachments can also be found throughout. The 1950 European Convention on Human Rights follows a similar structure to that of the UN Declaration of Human Rights and comes to the same points even quicker and even more decidedly. Article 2, which deals with the right to life, states in paragraph 1 that "[e]veryone's right to *life* shall be protected by law." (emphasis added) with exceptions extensively defined as severely restricted to necessary uses of force in defence of the self or in defence of the public order.[176] Article 5 continues with an extensive definition of the right to liberty, starting with "[e]veryone has the right to *liberty* and *security of person.*" (emphasis added) and containing extensive juridification for exceptions to this right.[177] Besides

[174] Article 6 ICCPR.
[175] Article 9 ICCPR.
[176] Article 2(2) ECHR: "Deprivation of *life* shall not be regarded as inflicted in contravention of this Article when it results from the *use of force* which is no more than absolutely necessary: (a) *in defence of any person from unlawful violence*; (b) *in order to effect a lawful arrest* or *to prevent the escape of a person lawfully detained*; (c) *in action lawfully taken for the purpose of quelling a riot or insurrection*.". (emphasis added)
[177] Article 5 ECHR: "1. *Everyone has the right to liberty and security of person.* No one shall be deprived of his *liberty* save in the following cases and in accordance with a procedure prescribed by law: (a) the lawful detention of a person after conviction by a competent court; (b) the lawful arrest or detention of a person for noncompliance with the lawful order of a court or in order to secure the fulfilment of any obligation prescribed by law; (c) the lawful arrest or detention of a person effected for the purpose of bringing him before the competent legal authority on reasonable suspicion of having committed an offence or when it is reasonably considered necessary to prevent his committing an offence or fleeing after having done so; (d) the detention of a minor by lawful order for the purpose of educational supervision or his lawful detention for the purpose of bringing him before the competent legal authority; (e) the lawful detention of persons for the prevention of the spreading of infectious diseases, of persons of unsound mind, alcoholics or drug addicts or vagrants; (f) the lawful arrest or detention of a person to prevent his effecting an unauthorised entry into the country or of a person against whom action is being taken with a view to deportation or extradition. 2. Everyone who is arrested shall be informed promptly, in a language which he understands, of the reasons for his arrest and of any charge against him. 3. Everyone arrested or detained in accordance with the provisions of paragraph 1 (c) of this Article shall be brought promptly before a judge or other officer authorised by law to exercise judicial power and shall be entitled to trial within a reasonable time or to release pending trial. Release may be conditioned by guarantees to appear for trial. 4. Everyone who is deprived of his liberty by arrest or detention shall be entitled to take proceedings by which the lawfulness of his detention shall be decided speedily by a court and his release ordered if the detention is not lawful. 5. Everyone who has been the victim of arrest or detention in contravention of the provisions of this Article shall have an enforceable right to compensation." (emphasis added)

articles on the protection of life and liberty, in its first protocol, the Protocol to the Convention for the Protection of Human Rights and Fundamental Freedoms, the convention starts out with the protection of property, by stating that "[e]very natural or legal person is entitled to the peaceful enjoyment of his *possessions*.".[178] (emphasis added) In other words, just as we have seen on the global level with the UN framework, on the European level too, we see that human rights documents reflect human nature in their protection of the interests of life, liberty and property.

Additionally, we can also discern a consistent pattern in the protection of these rights by extensive, additional prohibitions against especially egregious encroachments on these rights – such as through torture and slavery. In the case of the prohibition on torture, these can be found in the UN Declaration on Human Rights in article 5,[179] in article 7 of the ICCPR[180] and in article 3 of the ECHR.[181] In the case of prohibitions on slavery, these can be found in the UN Declaration on Human Rights in article 4,[182] in article 8 of the ICCPR[183] and in article 4 of the ECHR.[184] Furthermore, slavery and other types of forced labour are comprehensively and

[178] Article 1 ECHR Protocol I: "*Every natural or legal person is entitled to the peaceful enjoyment of his possessions. No one shall be deprived of his possessions except in the public interest and subject to the conditions provided for by law and by the general principles of international law.* The preceding provisions shall not, however, in any way impair the right of a State to enforce such laws as it deems necessary to control the use of property in accordance with the general interest or to secure the payment of taxes or other contributions or penalties.". (emphasis added)

[179] Article 5 UN Declaration on Human Rights: **"**No one shall be subjected to *torture* or to *cruel, inhuman or degrading treatment or punishment*." (emphasis added)

[180] Article 7 ICCPR**:** "No one shall be subjected to *torture* or to *cruel, inhuman or degrading treatment or punishment*. In particular, no one shall be subjected without his free consent to medical or scientific experimentation." (emphasis added)

[181] Article 3 ECHR: "No one shall be subjected to *torture* or to *inhuman or degrading treatment or punishment*." (emphasis added)

[182] Article 4 UN Declaration on Human Rights: "No one shall be held in *slavery* or *servitude*; *slavery and the slave trade shall be prohibited in all their forms*." (emphasis added)

[183] Article 8 ICCPR: "1. *No one shall be held in slavery; slavery and the slave-trade in all their forms shall be prohibited.* 2. *No one shall be held in servitude.* 3. (a) *No one shall be required to perform forced or compulsory labour*; (b) Paragraph 3 (a) shall not be held to preclude, in countries where imprisonment with hard labour may be imposed as a punishment for a crime, the performance of hard labour in pursuance of a sentence to such punishment by a competent court; (c) For the purpose of this paragraph the term "forced or compulsory labour" shall not include: (i) Any work or service, not referred to in subparagraph (b), normally required of a person who is under detention in consequence of a lawful order of a court, or of a person during conditional release from such detention; (ii) Any service of a military character and, in countries where conscientious objection is recognized, any national service required by law of conscientious objectors; (iii) Any service exacted in cases of emergency or calamity threatening the life or well-being of the community; (iv) Any work or service which forms part of normal civil obligations." (emphasis added)

[184] Article 4 ECHR: "1. *No one shall be held in slavery or servitude*. 2. *No one shall be required to perform forced or compulsory labour.* 3. For the purpose of this Article the term "forced or compulsory labour" shall not include: (a) any work required to be done in the ordinary course of detention imposed according to the provisions of Article5 of this Convention or during conditional release from such detention; (b) any service of a military character or, in case of conscientious objectors in countries where they are recognised, service exacted instead of compulsory military service; (c) any service exacted in case of an emergency or calamity threatening the life or wellbeing of the community; (d) any work or service which forms part of normal civic obligations." (emphasis added)

extensively defined as prohibited in the 1926 Convention to Suppress the Slave Trade and Slavery (subsequently supplemented with the 1956 Supplementary Convention on the Abolition of Slavery, the Slave Trade, and Institutions and Practices Similar to Slavery).[185] Similarly, torture is comprehensively and extensively defined as prohibited in the 1984 Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment.[186] Again we see that the framework on human rights protection, both on the global and regional level, is principally built around the protection of the interests of life, liberty and property.

Although these rights to life, liberty and property, as well as their negative inverse of torture and slavery, are defined differently in different legal systems, I believe their pervasive presence in political philosophy as well as in regional and international legal systems across time and space is not a historical coincidence, but rather, that it reflects a fundamental logic to legal systems which is demonstrated by both philosophy and theory, as well as by law and practice. This fundamental logic boils down to the point I have already made earlier, namely that on a fundamental level, what we call 'law' is a collection of codified private agreements which have been made pursuant to rational self-interest in order to increase self-determination through the prohibition on the use of force against life, liberty and property. These rights to life, liberty and property are not coincidental and subjective rights within one legal systems or another. Rather, they reflect fundamental universal laws of nature about the nexus between the

[185] *See generally* Convention to Suppress the Slave Trade and Slavery (hereinafter: "Slavery Convention"); and Supplementary Convention on the Abolition of Slavery, the Slave Trade, and Institutions and Practices Similar to Slavery (hereinafter: "Supplementary Convention on the Abolition of Slavery"; *see specifically* Article 1 Slavery Convention: "For the purpose of the present Convention, the following definitions are agreed upon: (1) *Slavery is the status or condition of a person over whom any or all of the powers attaching to the right of ownership are exercised.* (2) The slave trade includes all acts involved in the capture, acquisition or disposal of a person with intent to reduce him to slavery; all acts involved in the acquisition of a slave with a view to selling or exchanging him; all acts of disposal by sale or exchange of a slave acquired with a view to being sold or exchanged, and, in general, every act of trade or transport in slaves." (emphasis added);

[186] *See generally* Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment (hereinafter: "Torture Convention"; *see specifically* Article 1 Torture Convention: "For the purposes of this Convention, *the term "torture" means any act by which severe pain or suffering, whether physical or mental, is intentionally inflicted on a person for such purposes as obtaining from him or a third person information or a confession, punishing him for an act he or a third person has committed or is suspected of having committed, or intimidating or coercing him or a third person, or for any reason based on discrimination of any kind, when such pain or suffering is inflicted by or at the instigation of or with the consent or acquiescence of a public official or other person acting in an official capacity.* It does not include pain or suffering arising only from, inherent in or incidental to lawful sanctions." (emphasis added); *see also* Article 5 UN Declaration of Human Rights: "No one shall be subjected to *torture* or *to cruel, inhuman or degrading treatment or punishment.*" (emphasis added); Article 3 ECHR: "No one shall be subjected to *torture* or to *inhuman or degrading treatment or punishment*.". (emphasis added); Article 7 ICCPR: "No one shall be subjected to *torture* or *to cruel, inhuman or degrading treatment or punishment.* In particular, no one shall be subjected without his free consent to medical or scientific experimentation." (emphasis added)

biological nature of us as *homo sapiens* and the social nature of our human civilization. Given that our social life is ultimately formed by our biological life, the social can only function when the biological prerequisites of life, liberty and property are protected from force. As discussed in Section 3.2, Darwinian evolution, that universal law of biological nature, has selected for those individuals with the burning desire to fight for their survival when their lives, liberty and property are threatened. In other words, the reason we find these same rights throughout theory and practice is because they are natural. They are the laws of our societies not despite but because they are derived from nature.

Many societies have tried acting against these laws of nature and they have failed the test of time. They were simply unnatural. When a society allows for the widespread exercise of force against life, liberty and property, then this society will, in a best case scenario, be slowly outcompeted by a society which does protect these interests, because in this latter society, the non-zero-sum game nature of this society constantly creates new value. In a worst case scenario, such a society which allows for the widespread exercise of force against life, liberty and property, will become a completely zero-sum game society, wherein every bit of value needs to be extracted from someone else and thus, as a society, it turns into a death spiral of extraction. Laws cannot be arbitrary. Ultimately, they need to reflect our human nature.

In sum, this section has built on the findings of Section 3.2 on the laws of nature and has taken them to their logical conclusions; the laws of men. The laws of men are such that agreement is found on the mutual right to self-determination among participants to the agreement and this includes the prohibition of the use of force against life, liberty and property. Moreover, it has been argued that the reason why these interests and rights to life, liberty and property are found both in theory and practice, in political philosophy and in law, is because they are not coincidental, but rather, because they reflect laws derived from nature. In the next section, I will move from the laws of individual men to the laws of their collective expression as peoples.

3.4 On the Laws of States

At some point, these groups would naturally become too large to maintain peace and security without a central force which would protect the right to self-determination for the participants to the agreement through the prohibition of the us of force. Although these groups might have previously been able to self-correct transgressions of the agreement, as the groups of people

became larger and social interactions became more anonymous, there came a natural and logical need for a central force to enforce the agreement - a State. The *raison d'être* of the State is hence to preserve the *tranquilitas ordinis, i.e.*, the State is the securer of the vital interests of the individual and of peace and security in a society. In order to do this, the State must assume a monopoly on the use of force with which it can act as an arbiter against transgressions on the prohibition on the use of force. A Leviathan is born. The Leviathan ("לִוְיָתָן") of Hobbes receives its name from the mythical monster mentioned throughout the Tanakh.[187] It is fear in its absolute formand Hobbes imagines the monopolization of force by the State in its image.[188]

Individuals living in the State therefore have to, through the (implicit) acceptance of the so-called social contract, accept the Leviathan's monopoly on the use of force. In the Mishnah, one of the first written commentaries on the Oral Torah, one of the oldest justifications is given for this great force which needs to be embodied by the State. In the Ethics of Our Fathers, it says: "*Pray for the welfare of the government, for were it not for the fear of it, men would swallow one another alive*".[189] Hobbes clearly echoes this sentiment when he states in Chapter XIII, Of The Natural Condition of Mankind, Out of Civil States that: "There Is Alwayes Warre Of Every One Against Every One Hereby it is manifest, *that during the time men live without a common Power to keep them all in awe, they are in that condition which is called Warre; and such a warre, as is of every man, against every man*.".[190] (emphasis added)

In order to take people out of this state of nature, people need to be kept 'in awe' by the awesome power of a State.[191] Through the social contract they accept the monopoly on the use of force by the State to enforce the rules – notably the rules to protect the right to self-

[187] Book of Job 3:8, 40:15–41:26; Book of Amos 9:3, Book of Psalms 74:13–23, 104:26; Book of Isaiah 27:1.
[188] *See e.g.* Book of Jobs 41, at 12-34: "I will not fail to speak of Leviathan's limbs, its strength and its graceful form. Who can strip off its outer coat? Who can penetrate its double coat of armor[b]? Who dares open the doors of its mouth, ringed about with fearsome teeth? Its back has[c] rows of shields tightly sealed together; each is so close to the next that no air can pass between. They are joined fast to one another; they cling together and cannot be parted. Its snorting throws out flashes of light; its eyes are like the rays of dawn. Flames stream from its mouth; sparks of fire shoot out. Smoke pours from its nostrils as from a boiling pot over burning reeds. Its breath sets coals ablaze, and flames dart from its mouth. Strength resides in its neck; dismay goes before it. The folds of its flesh are tightly joined; they are firm and immovable. Its chest is hard as rock, hard as a lower millstone. When it rises up, the mighty are terrified; they retreat before its thrashing. The sword that reaches it has no effect, nor does the spear or the dart or the javelin. Iron it treats like straw and bronze like rotten wood. Arrows do not make it flee; slingstones are like chaff to it. A club seems to it but a piece of straw; it laughs at the rattling of the lance. Its undersides are jagged potsherds, leaving a trail in the mud like a threshing sledge. It makes the depths churn like a boiling caldron and stirs up the sea like a pot of ointment. It leaves a glistening wake behind it; one would think the deep had white hair. Nothing on earth is its equal— a creature without fear. It looks down on all that are haughty; it is king over all that are proud."
[189] *See, e.g.*, Ethics of Our Fathers: Avot 3:2 Rabbi Chanina, deputy to the high priest ("*kohanim*"): "Pray for the welfare of the government, for were it not for the fear of it, men would swallow one another alive.".
[190] *See* Hobbes, *Leviathan*, Chapter XIII.
[191] *See* Hobbes, *Leviathan*, Chapter XIII.

determination through the protection of the rights to life, liberty and property. There are two main parts to this social contract with regards to peace and security. First, the individual has to accept that the State's use of force is legitimate *vis-à-vis* himself (vertical legitimacy).[192] Second, the individual has to accept that he is no longer authorized to unilaterally protect his vital interests of life, liberty and property *vis-à-vis* other individuals (horizontal legitimacy).[193] The surrender of the individual's natural right to act unilaterally in the protection of his vital interests is the quintessential precondition for individuals to transcend the state of nature in which they lived prior to the State and its monopolization of the use of force.

However, the State never takes away the right to act in self-preservation completely.[194] Instead, nearly every domestic legal order, mindful of the fact that the State cannot always be capable of protecting (or may not always be willing to protect) the vital interests of the individual, allows the individual to use force to act in some sort of self-preservation.[195] Monopoly, in this sense, is a fiction used to facilitate academic discussions, but it should not be taken as a factual absolute. The State never completely monopolizes the use of (just) force and always leaves part of the natural right of people to act in self-preservation in the hands of the individuals themselves.[196] It is this remainder of one's natural right to act in self-preservation which is referred to in domestic law systems as 'self-defence'.[197] This right to act in self-defence can be found as legal rights in virtual every legal to one degree or another.[198] It has been acknowledged in so many domestic legal orders that it rightly qualifies as natural law.[199]

This law of the right to self-defence is however broader than the mere declaration of a legal right to self-defence. Rather, nearly every domestic legal order, mindful of the fact that unilateralism ought to be restricted to a sufficient degree in order to be able to transcend the

---

[192] *See* Hobbes, *Leviathan*, Chapter XIII; *see also* Locke, *Second Treatise of Government*, Chapter VIII, sect. 97: "And thus every man, by consenting with others to make one body politic under one government, puts himself under an obligation, to every one of that society, *to submit to the determination of the majority, and to be concluded by it* […].", Chapter IX, sect. 128: "For in the state of nature, to omit the liberty he has of innocent delights, a man has two powers. The first is to do whatsoever he thinks fit for the preservation of himself […] The other power a man has in the state of nature, is the power to punish the crimes committed against that law. *Both these he gives up, when he joins in a private, if I may so call it, or particular politic society, and incorporates into any commonwealth, separate from the rest of mankind*.", Chapter IX, sect. 129-130: "The first power, viz. of doing whatsoever he thought for the preservation of himself, and the rest of mankind, he gives up to be regulated by laws made by the society […] Secondly, *The power of punishing he wholly gives up* […]". (emphasis added)
[193] *Id.*
[194] *See* P. Haggenmacher, *Self-Defence as a General Principle of Law and its Relation to War, in* A. Eyffinger, A. Stephens & S. Muller (Ed.), Self-Defence as a Fundamental Principle, p. 14-18 (2008).
[195] *Id.*
[196] *Id.*
[197] *Id.*
[198] *Id.*
[199] *Id.*

state of nature, connects this right to certain specific conditions and restrictions which can be also be found universally.[200] Most legal orders connect the right to self-defence to some degree to the normative restraints of necessity, proportionality and immediacy.[201]

As such, most domestic law systems exclude the right to act in pre-emptive or preventive self-defence because it is deemed unnecessary to punish mere intentions and ideas which have not yet resulted in (substantive) actions.[202] Broadly speaking, the temporal aspect of self-defence can be divided into four categories; *reactive self-defence* (self-defence in direct response to an attack against life, liberty or property and which has already struck),[203] *interceptive self-defence* (self-defence in anticipation of an attack against life, liberty or property which is already underway, but which has not yet struck),[204] *pre-emptive self-defence* (self-defence in anticipation of an attack against life, liberty and property which is not yet underway, but which is expected to be launched imminently due to active preparations)[205] and *preventive self-defence* (self-defence in anticipation of an attack against life, liberty and property which has not yet been launched and is not yet imminent, but for which there exist general preparations).[206] Generally speaking, most domestic law systems prohibit preventive- and most types of pre-emptive self-defence and only allow for reactive- and some types of interceptive self-defence.[207] Given that a strong State can punish those who actually *engage* in use of force to a sufficient degree in order establish an effective deterrence, both through a special and a general prevention of (potential) aggressors, individuals no longer need to take such precautions. Dealing with non-immediate threats therefore ought to become the task of the State, whereas previously it would certainly behoove any individual to strangle any potential future aggression at birth. Indeed, throughout much of human history, the killing of babies and boys who might otherwise grow up to become hostile men has often been the more pragmatic course of action.

---

[200] *Id.*
[201] *Id.*
[202] *Id.*
[203] *See e.g.* T. Ruys, 'Armed Attack' and Article 51 of the UN Charter Evolutions in Customary Law and Practice, p. 253-254 (2010). Although these categories can not always be strictly separated and although many authors use different terms and different lines of separation when discussing self-defence, these categories
provide a terminology which will help to comprehend the concept of the temporal aspect or *rationae temporis* of self-defence.
[204] *See* Ruys, 'Armed Attack' and Article 51 of the UN Charter Evolutions in Customary Law and Practice, p. 253-254.
[205] *Id.*
[206] *Id.*.
[207] *See* Haggenmacher, *Self-Defence as a General Principle of Law and its Relation to War*, p. 14-18.

In addition to excluding the right to act in self-defence preventively and pre-emptively, most domestic law systems exclude the right to act punitively as well, due to such action being considered disproportionate to the threat faced.[208] When the State has monopolized the use of force, this is certainly so. Prior to this monopolization however, harsh punitive self-defence would not necessarily be considered disproportionate to the aggression that is being punished, as it could be considered necessary to establish effective deterrence. After all, if an aggressor is only punished for the damage he has caused when he is caught by the victim, but can get away unpunished for the times he cannot be caught by the victim, then no effective deterrence for future aggression can be established. The State wields a lot more power to catch aggressors and can therefore change the cost/benefit analysis of a potential aggressor with less punishment. Punitive self-defence in this sense is a punishment not just for the damage when he is caught, but especially also for all the times when he is not. When the State does become the one tasked with the establishment of effective deterrence against the use of force, the individual no longer has the need to engage in such harsh punitive self-defence, because the enforcement improves. For the same reason as punitive self-defence is not allowed in most domestic law systems, most law systems also exclude the right to act after the threat has already passed. By then the action would be of a retaliatory nature and constitute revenge rather than immediate self-defence. Prior to the monopolization of the use of force by the State, vengeance would be deemed necessary in order to establish effective deterrence. If you're not the biggest and baddest on the block, then you're only inviting future aggression. *Nemo me impune lacessit*.

These normative restraints on the right to self-defence are so inextricably linked to the general notion of self-defence in domestic law systems that they are to be considered an addendum to the right to self-defence as a natural law.[209]

However, it must be noted that notions of necessity, proportionality and immediacy are also closely connected to how well the State performs in its principal task of protecting the individual's most vital interests – namely life, liberty and property.[210] After all, a prohibition on the use of force is only possible if this force is *effectively* monopolized in the hands of State organs. Otherwise, effective deterrence from the use of force is not established and the

[208] *Id.*
[209] *Id.*
[210] A. Eyffinger, *Self-Defence or the Meanderings of a Protean Principle, in* A. Eyffinger, A. Stephers & S. Muller (Ed.), Self-Defence as a Fundamental Principle, p. 115 (2008).

legitimacy of the State and its force comes into question. The State thus needs to maintain effective control over its sovereign spaces.[211]

Moreover and conversely, if the State were to provide no real effective protection of the individual's vital interests and fails to create the necessary effective deterrence, then it cannot simply be expected of the individual that he accepts grave threats to his life, liberty or property. The social contract is no suicide pact.[212] The legitimacy of the State as the guarantor of the *tranquilitas ordinis* is not a black-or-white notion. Rather, many shades of grey exist and the normative restraints on self-defence as discussed above respond accordingly. In legal orders where effective deterrence and the monopolization of the use of force by the State is strong, there are stronger restraints on the right to self-defence. In legal orders where effective deterrence and the monopolization of the use of force by the State is weak, there are weaker restraints on the right to self-defence. In legal orders where effective deterrence and the monopolization of the use of force by the State is somewhere between strong and weak, the restraints on the right to self-defence are somewhere between strong and weak. In this sense, the monopolization of the use of force by the State and the normative restraints on the right to self-defence by the individual are communicating vessels.

This principle of the monopolization of the use of force by the State and the normative restraints on the use of force by the individual is famously demonstrated by the Texas 'trespassers will be shot on sigh'- scenario. Given that, as the expression goes; 'Everything's bigger in Texas', this too is the case for estates. In the classic Texas scenario, the land owners live remotely from the major cities on large private estates where the arm of the law cannot always reach to provide effective deterrence to protect the individual's vital interests of life, liberty and property. Rather, it is the land owner himself who ultimately remains responsible for the protection of his vital interests. Therefore, (sometimes) he can be the sole sovereign on his land when the official sovereign cannot provide effective deterrence from aggression. He can 'take the law in his own hands', because until the State sovereign arrives, the individual is the sovereign. Especially in the olden days when there were no phones, let alone cyberspace, for all intents and purposes, the individual needn't expect the State to provide any protection whatsoever, despite formally being under its sovereignty. Moreover, what is important to note

[211] It is this effective control over the sovereign space of cyberspace which is the topic of Chapters 4-6.
[212] *See* Hobbes, *Leviathan*, Chapter XIV: "*a man is forbidden to do, that, which is destructive of his life*, or taketh away the means of preserving the same; and to omit, that, by which he thinketh it may be best preserved.". (emphasis added)

in this situation, is that the State generally *allows* for this type of action.[213] The State in these weaker legal orders is aware that it has greater limitations to its monopolization of the use of force than do most legal orders and the normative restraints on the right to self-defence therefore become more lenient corresponding to the degree of this limitation.[214] Therefore, particular types of self-preservation which are often forbidden in strong legal orders, can become legitimate in weaker legal orders, because of the communicating vessels of the prohibition on the use of force and the right to act in self-defence.[215] Trespassers will hence be shot on sight. Effective deterrence to threats against life, liberty and property is to be created by either the State or by the individual. If it is not by the one, then it is by the other.

This general notion, which can be defined as the conditionality of the surrender of parts of the individual's natural right to act unilaterally in self-preservation, upon the willingness and ability of the central authority to provide effective protection of the individual's most vital interests to life, liberty and property, is the second addendum to the right to self-defence as a natural law.[216]

In sum, the right to act in self-defence has been accepted as deriving from the natural law to act in self-preservation. In order to transcend the state of nature, the State assumes a monopoly on the use of force pursuant to the social contract. This includes both the acceptance by the individual of horizontal- and vertical legitimacy of the State's use of force. It is hence the State which takes over the task of creating effective deterrence from and for the individual. Therefore, the right to use force in self-preservation is principally taken over by the State. However, due to the fact that the State cannot always provide effective deterrence against aggression against life, liberty and property, the State never takes away the right to use force to act in self-preservation completely. Rather, it strips the right to self-preservation down to the right to self-defence, which includes the normative restraints of necessity, proportionality and immediacy and prohibits preventive, pre-emptive and punitive self-defence. However, these normative restraints remain conditional upon the need for the individual to protect one's vital interests of life, liberty and property and to act in self-preservation when this is necessary. Generally speaking, the State takes away this necessity. When it fails to do so, the individual can reclaim the right to protect his vital interests of life, liberty and property. In Chapters 5 and

[213] *See* Eyffinger, *Self-Defence or the Meanderings of a Protean Principle*, p. 115.
[214] *Id.*
[215] *Id.*
[216] *See* Haggenmacher, *Self-Defence as a General Principle of Law and its Relation to War*, p. 14-18.

6 these rights to life, liberty and property and the principles discussed in this section will be connected to the domain of cyberspace. The next section will first take these findings on the monopolization of the use of force by the State and the remaining right to self-defence with its addenda of conditional normative restraints by the individual to the level of international relations.

3.5 On the Laws of the International Order

The previous sections have described the individual's right to self-defence as deriving from human nature's innate drive to act in its self-preservation and they have described how the State becomes tasked with (parts of) this protection through the social contract. Further, the right to self-defence has been described as a natural law to which two addenda exist. It has been explained that the *raison d'être* of the State is the protection of the vital interests of the individual – namely life, liberty and property - due to the assumption by the State of the monopoly on the use of force as derived from the drive of humans to act in self-preservation for the protection of these same interests. Hence, it is posited that through the monopolization of the use of force and the creation of the State, that an innate moral and legal duty is created for the State to protect the individual's vital interests. This implies that the State does not merely protect the individual's vital interests of life, liberty and property against other individuals living in that State, but that the State itself may and also must act in self-defence against external aggressors, *i.e.*, against other States or against non-State aggressors and that it must do so in the protection of its citizens and itself.

In order to explain the legitimacy of this right to self-defence for the State itself, the domestic analogy for international relations is commonly used. There are many different definitions and interpretations for the term 'domestic analogy', but for the purposes of this dissertation, I will put it here in its simplest grammatical interpretation; the domestic analogy for international relations is the idea that States relate to each other in international society in a manner analogous to the way that individuals do so in domestic society.

There are several justifications for the validity of using the domestic analogy to describe international relations and moral judgments about interstate behavior. As the previous section has set out, the *raison d'être* of a State is the protection of the vital interests of the individual of life, liberty and property. In this sense, the State's right to self-defence is inherent, because it is part of the social contract which is created between the individual and the State. It is inherently

inherited. This view, which reasons from a responsibility of the State, has some basis in history. Historically speaking, the primary task of the State has been to protect the *tranquilitas ordinis* for the individual, not merely between individuals in the State, but also and especially beyond the State, from external aggression. The legitimacy of any regime has depended on this, regardless of time and place. Even in the absence of the explicit consent of the governed through democratic elections, governments have recognized that the implicit consent of the governed depends on the protection of peace and security - within the State through the creation of law and order and especially also beyond the State through self-defence against external aggression. It is the primary task of any State. Failure to do so will inevitably result in a decrease in legitimacy and an eventual revolt or overthrow. Even though historically speaking, the rights to life, liberty and property were by no means as protected as they are today (they could perhaps best be described as mafia-esque protection rackets whereby the only protection provided was against an even more exploitative ruler) and even though there is much leeway before a State which is unable or unwilling to protect these vital interests faces revolt or overthrow (most States have treated their citizens as little more than tax cattle to be milked dry, but not to be slaughtered), ultimately speaking, the legitimacy and continued survival of any regime depends on a basic protection of life, liberty and property. This State's inheritance of individual interests, leads us to the second justification for the validity of using the domestic analogy for international relations. Given that, as we discussed in Section 3.2, the right to self-defense and the protection of life, liberty and property is *instinctu naturae* in humans, it is therefore also inborn in the State as States, according to this explanation, can be best understood to be 'human families'. This notion of (nation) States as being human families is heavily reflected in international law.[217] Walzer on the other hand, takes a somewhat different view to come to the same conclusion. In his view, the right to self-defence of the State does not merely derive from the protection of the individual or the collection of individuals, but also from the State's moral duty to protect the community which is created, formed and maintained by these individuals.[218] It is a claim to (property) rights to a common life of infrastructures, of common organization

[217] *See, e.g.,* preamble ICCPR: "Considering that, in accordance with the principles proclaimed in the Charter of the United Nations, recognition of the inherent dignity and of the equal and inalienable rights of *all members of the human family* is the foundation of freedom, justice and peace in the world". (emphasis added); preamble ICESCR: "Considering that, in accordance with the principles proclaimed in the Charter of the United Nations, recognition of the inherent dignity and of the equal and inalienable rights of *all members of the human family* is the foundation of freedom, justice and peace in the world". (emphasis added)

[218] M. Walzer, Just and Unjust Wars, p. 53-54 (2006): "The moral standing of any particular state depends upon the reality of the common life it protects and the extent to which the sacrifices required by that protection are willingly accepted and thought worthwhile. If no common life exists, or if the state doesn't defend the common life that does exist, its own defense may have no moral justification. But most states do stand guard over the community of their citizens, at least to some degree: that is why we assume the justice of their defensive wars.".

and of common community.[219] Consequently, Walzer does not merely look at the moment of the creation of the State and the subsequent innate desire for its self-preservation, but also at the State's development and its social institutions preceding and following the moment of the State's creation. (Chapters 5 and 6 deal with the creation of such common properties and infrastructures.) This view seems to bridge a gap between the previous three justifications for the domestic analogy and the fourth justification, which can be regarded as the moral opposite to the previous justifications. Whereas the previous three justifications for the right of self-defense for the State can be regarded as bottom-up approaches of legitimacy, this fourth view is called 'statism' and it is the theory that States attain a right to self-defence top-down and *sui generis* through their sovereign existence.[220] Similar to the way in which individuals need to protect their vital interests for their self-preservation, so do States. The difference between statism and these other views is that statism is not reliant on the legitimacy provided by the people living in that State. This fourth justification, which according to Téson is "conceptually and morally wrong in this traditional form and too extreme even in its more benign versions", is on the decline and arguably rightly so.[221] However, it is important for the domestic analogy to regard the State both as the representative body of the interests of its people and as an independent entity with its own innate desire for self-preservation which may sometimes be in conflict with the interests of individual people. The clearest example of this conflict is when the State has to sacrifice the lives of some of its soldiers to protect the lives of most of its civilians from aggression from within or from without. Self-defence is hence the *right* and the *must* of any State.

Regardless of the justification, these philosophers share common ground in their theories in that they agree that States attain their inherent right to self-defence in the international legal order analogous to the way that individuals attain their right to self-defence in domestic legal orders. And it is the correct view. The right to self-defence of the State should be closely connected to the protection of the State's vital interests as these interests too are natural. We have seen in Section 3.3 that the vital interests of the individual are life, liberty and property. Analogously, the vital interests which the State needs to defend ought to connect to the State's existence, freedom and property. It is hence unsurprising that the vital interests

[219] *See generally infra* Chapters 5 and6, which deal with the creation of such common properties and infrastructures.
[220] *See* F. Teson, *A Philosophy of International Law* (1998), p. 40-41.
[221] *See* Teson, *A Philosophy of International Law,* p. 39. The interests of the people should be the goal to pursue and the State the instrument to do so, not the other way around.

which the State needs to defend pursuant to international law and philosophy are its sovereign existence, political independence and territorial integrity, being, analogously and respectively, the collective expressions of life, liberty and property for the State.[222]

Sovereign existence in this sense refers to the concrete existence or survival of the State, whereas political independence and territorial integrity comprise this concrete existence". *Political independence* refers to the freedom of decision-making or self-direction customarily demanded by state officials". *Territorial integrity* refers to "the geographical extension of a state's defined territory".

Beyond protection of these interests in philosophy and theory by the most authoritative political philosophers, we also find these same interests protected as rights in law and practice in the most authoritative legal documents. The 1945 Charter of the United Nations, the foundational document of the most recent attempt to create an international legal order, states in article 1(1) that its primary purpose is "To maintain international peace and security".[223] In other words, the first-mentioned purpose of the UN Charter is to protect the *tranquilitas ordinis* in the international relations between States, analogous to how the primary purpose of domestic legal orders is to protect the *tranquilitas ordinis* in domestic relations between individual persons.

It should be noted here that the *tranquilitas* in international relations has historically been anything but *ordinis* and that it has been more akin to the state of nature in which individual people lived prior to the creation of the State.[224] Unsurprisingly, the concepts of State sovereignty and Balance of Power have historically attributed States a right to use force as a

---

[222] *See* Walzer, *Just and Unjust Wars*, at 54-55: "*The protection extends not only to the lives and liberties of individuals but also to their shared life and liberty*, the independent community they have made, for which individuals are sometimes sacrificed. […] And given a genuine "contract"[,][sic] it makes sense to say that *territorial integrity and political sovereignty can be defended in exactly the same way as individual life and liberty*. It might also be said that a people can defend its country in the same way as men and women can defend their homes, for the country is collectively as the homes are privately owned. *The right to territory might be derived, that is, from the individual right to property.* (emphasis added)

[223] 1945 Charter of the United Nations (hereinafter: "UN Charter"), 1 UNTS XVI (1945), Article 1(1): "To *maintain international peace and security*, and to that end: to take effective collective measures for the prevention and removal of threats to the peace, and for the suppression of acts of aggression or other breaches of the peace, and to bring about by peaceful means, and in conformity with the principles of justice and international law, adjustment or settlement of international disputes or situations which might lead to a breach of the peace." (emphasis added).

[224] *See, e.g.*, Locke, *Second Treatise of Government*, Chapter II, sect. 14: "[…] *all princes and rulers of independent governments all through the world, are in a state of nature*". (emphasis added)

means of furthering interests and as a means of redressing grievances, analogous to such rights for individuals in their respective state of nature.

This has however changed over time and in stages. The inception of the general inadmissibility of the use of force in international relations dates back to the beginning of the 20th century. The 1920 Covenant of the League of Nations was the first attempt to regulate the unilateral use of force through general prohibitions (as opposed to previous *jus in bello* prohibitons) by declaring that within the League of Nations, members accepted their obligations "not to resort to war".[225] Similarly, the 1928 International Treaty for the Renunciation of War as an Instrument of National Policy (Kellogg-Briand Pact) provided that members to the treaty "condemn recourse to war for the solution of international controversies".[226] States thus agreed not to use war as an instrument of national policy. In other words, they agreed not to use force for offensive purposes, but instead, only for defensive purposes. Such agreements imply respect for certain interests of other States.

However, World War II soon demonstrated that international laws and agreements, just as national laws and agreements, have little practical value without an effective means to enforce them. In the absence of an international Leviathan who can use force which is just, force will also be used when it unjust. Reservations from doing so will again be merely of a pragmatic nature.[227] Additionally, during the 20th century, the term 'war' contained in both provisions came in disuse, thereby creating a grave loophole in the agreements. The 1945 Charter of the United Nations attempted to remedy these issues and represents the starting block for any current discussion on the international use of force. In article 2(4) of the UN Charter, we find the prohibition on the use of force within the international legal order. It reads: "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.".[228] (emphasis added) The UN prohibition on the use of force thus broadened the prohibition on forceful action to a general prohibition on the use (or threat) of 'force' – instead of the more restrictive criteria of a declaration of war.

Additionally, the UN Charter also attempted to create an international Leviathan of sorts with the creation of the UN Security Council, which was created with the authority and the

[225] Preamble, 1920 Covenant of the League of Nations, ATS 1 (1920).
[226] 1928 International Treaty for the Renunciation of War as an Instrument of National Policy, 94 LNTS 57 (1928).
[227] *See supra* Section 3.2.
[228] Article 2(4) UN Charter.

legitimacy to enforce (especially egregious) transgressions to the prohibition on the use of force in order to maintain peace and security (*i.e. tranquilitas ordinis*).[229]

Article 2(4) UN Charter, which is now widely regarded as customary international law and even enjoys the status of *jus cogens*, also reflects an acknowledgment among the founders of the United Nations that in order to maintain the *tranquilitas ordinis* in international relations, it needs to protect the vital interests of the member States. Two of these vital interests are codified in article 2(4) of the UN Charter; territorial integrity and political independence – the international variants of property and liberty – which, as just discussed, comprise the concrete existence of sovereignty.

Just as we have seen in Section 3.3 on the protection of the interests of life, liberty and property, the recognition of the international variants of these interests as being vital to States has been enumerated throughout the international legal system – such as in the Definition of Aggression,[230] the Declaration on Friendly Relations[231] and in the Declaration on the Non-Use of Force,[232] where special consideration is attributed to these rights.

Because of these vital interests - and analogous to the individual -, the State may, in principle, protect itself by any and all means, *i.e.*, he may use force pre-emptively, preventively, punitively or in any manner deemed necessary for self-preservation in the great chaos and arguably anarchical nature of international relations.[233] As mentioned above, this has historically also been the case. With no international monopolization of the use of force through a super-State, let alone a police force or even an agreed upon sheriff with or without a posse,

[229] Article 24 UN Charter: "In order to ensure prompt and effective action by the United Nations, *its Members confer on the Security Council primary responsibility for the maintenance of international peace and security, and agree that in carrying out its duties under this responsibility the Security Council acts on their behalf.* In discharging these duties the Security Council shall act in accordance with the Purposes and Principles of the United Nations." (emphasis added); Article 25 UN Charter: "The Members of the United Nations *agree to accept and carry out the decisions of the Security Council* in accordance with the present Charter" (emphasis added), 39 UN Charter: "*The Security Council shall determine the existence of any threat to the peace, breach of the peace, or act of aggression* and shall make recommendations, or decide what measures shall be taken in accordance with Articles 41 and 42, to maintain or restore international peace and security.". (emphasis added)
[230] Article 1 Definition of Aggression: "Aggression is the use of armed force by a State against the *sovereignty, territorial integrity or political independence* of another State […]". (emphasis added)
[231] Principle f Declaration on Friendly Relations: "Each State enjoys the rights *inherent in full sovereignty* […] The *territorial integrity* and *political independence* of the State are inviolable […] Each State has *the right freely to choose and develop its political, social, economic and cultural systems*. (emphasis added)
[232] Declaration 1(7), Declaration on the Non-Use of Force: "States have the duty to abstain from armed intervention and all other forms of interference or attempted threats against the *personality of the State* or against its *political, economic and cultural elements*". (emphasis added)
[233] *See supra* Section 3.2.

none are responsible for the protection of these vital State interests but the States themselves. Unilateralism reigns supreme.

As we have seen in Section 3.4 however, the right to act unilaterally in the protection of one's vital interests can also be outsourced. Individuals have, often with great success, contracted out parts of their right to use force in the protection of their vital interests, in exchange for improved protection of these interests, provided for by the State. By giving up the unilateral protection of these interests, individuals in domestic societies have managed to transcend the state of nature in which they lived prior to the State. As described previously in this section, States have started to do the same since the beginning of the 20th century. Through the signing of the UN Charter, States have agreed to "confer on the Security Council primary responsibility for the maintenance of international peace and security" and to accept that "the Security Council acts on their behalf".[234] Thereto, States agreed to "accept and carry out the decisions of the Security Council" and to "refrain in their international relations from the threat or use of force", corresponding, respectively, to the vertical and horizontal legitimacy which we have also seen in Section 3.4 on the obligations of the individual to the State pursuant to the social contract.[235] Members of the international community have thus accepted to surrender their rights to unilateralism *vis-à-vis* each other and have accepted the authority of the UN Security Council *vis-à-vis* them – analogous to what has happened in domestic law systems.[236] The UN Security Council has thereby become authorized and tasked to "determine the existence of any threat to the peace, breach of the peace, or act of aggression" and to "decide what measures shall be taken in accordance with Articles 41 and 42, to maintain or restore *international peace and security*".[237] (emphasis added)

States thus agreed to surrender certain elements of their natural right to act in self-preservation to the UN Security Council in order to transcend the state of nature of international relations in which they had previously lived and they have done so in a way which is analogous to the way this has happened in domestic law systems. Analogous to domestic law systems, in the international law system, it is the remainder of this right to use force in self-preservation which is called self-defence. In Article 51 UN Charter the right to self-defence is codified.[238] It encapsulates the tension between the inherent, natural right of States to use force in acts of self-

[234] Article 24(1) UN Charter.
[235] Article 25 UN Charter.
[236] *See supra* Section 3.4.
[237] Article 39 UN Charter.
[238] Article 51 UN Charter

preservation and the outsourcing of this right to the international Leviathan, the UN Security Council. It reads: "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.".[239] (emphasis added) We see that the right to self-defence is being described as 'inherent'. In other words, the right to self-defence is not considered to exist as a matter of legal right, constituted by the UN Charter, but as a matter of natural fact. It is not a legal right constituted, but a natural right recognized and codified by positive international law.

Conversely, the second part of the first sentence of Article 51 points us to the fact that, similar to the domestic community, the central governing body of the international community, the UN Security Council, not only attains the *right* to use force legitimately, but also the *duty* to do so – especially when in the protection of the sovereign existence, political independence and territorial integrity of its member States is at stake. The surrender of the States' right to act unilaterally in self-preservation is thus also conditional upon the UN Security Council's ability to establish the effective deterrence which can render future unilateralism unnecessary. Although passionate debates can be waged as to the degree to which the UN Security Council has managed to become an international Leviathan which has taken away the necessity for unilateralism, it is beyond any reasonable doubt that the international legal order ought to be characterized as a weaker legal order than are most advanced domestic legal orders. It would therefore certainly behoove States who's sovereign existence, political independence or territorial integrity are under threat of force, to monitor the UN Security Council's performance closely. If the UN Security Council demonstrates that it is unable or unwilling to protect a State's vital interests, then this State may take matters into his own hands and arguably also sooner than would be the case in a strong legal order. Moreover, as explained in Section 3.4, pursuant to the second addendum to the right to self-defence as natural law, such action could be considered legitimate as well. Just as the social contract in the domestic legal order is no suicide pact, neither is the UN Charter in the international legal order.

In sum, States inherit their 'inherent' right to self-defence analogous to and derived from the natural right to self-defence of the individuals whose interests it protects. This right is thus closely connected to the protection of the vital interests of life, liberty and property and consists, pursuant to the domestic analogy, respectively, of sovereign existence, political independence

[239] Article 51 UN Charter.

and territorial integrity. In principle, States therefore also inherit an unlimited right to act unilaterally in self-preservation - especially when it comes to the protection of their sovereignty, political independence or territorial integrity. Analogous to individuals in domestic law systems however, a large part of this right has over time also been contracted out to the UN Security Council in the international law system through the UN Charter and subsequent developments. However, this surrender of one's right to act in self-preservation can also not equate a suicide-pact and thus remains, to some degree, conditional upon the Security Council's success in protecting the State's vital interests of sovereign existence, political independence and territorial integrity. Effective deterrence to threats against the life, liberty and property of the State is to be created by either the State or by the individual. If it is not by the one, then it is by the other.

3.6 Conclusion

This Chapter started with the poem *The Law of the Jungle* by Rudyard Kipling from his book *The Jungle Book*.[240] In this book, Kipling uses a collection of stories with anthropomorphized animals to teach moral lessons. In the specific poem included here, Kipling teaches the rules of a pack of wolves. Such laws from nature have formed the basis for this chapter.

In Section 3.2, I started with the laws of nature. In nature, every life form acts according to its perceived self-interest in order to survive and to reproduce. Doing so is the *conditio sine qua non* for its continued existence and reproductive success in an environment where there is competition for scarce resources - such as food and reproductive opportunities. In this competition, the individual naturally and logically bears the ultimate responsibility for his self-preservation and may do so in any way necessary including through the use of force. Because of this, in the state of nature man must be wolf to man.

In Section 3.3, I have explained how the laws of nature, naturally and logically lead to the laws of men. Given that the war of all against all in the state of nature makes "the life of man, solitary, poor, nasty, brutish, and short.",[241] there is good reason to form agreements with other men on a mutual right to self-determination and thereto, to prohibit the use force of force against the life, liberty and property of participations to the agreement. In this section, I have also explained why I believe that the reason why these interests and rights to life, liberty and

[240] R. Kipling, The Jungle Book (1894), The Law of the Jungle.
[241] *See* Hobbes, *Leviathan*, Chapter XIII.

property are found both in theory and practice, in political philosophy and in law, is because they are not coincidental social rules, but rather, that it is because they reflect laws derived from our biological nature.

In Section 3.4, I have explained how the laws of men and the laws of peoples, naturally and logically lead to the laws of States. As groups of people become larger, the increasingly complex and anonymous nature of their societies requires a monopolization on the use of force in order to create effective deterrence against potential transgressors of the agreements on the mutual right to self-determination and the prohibition on the use of force against life, liberty and property. Thereto, individuals living in the State agree, pursuant to the social contract, to transfer part of their natural right to act in self-preservation over to the State. More specifically, they agree to surrender their right to act in preventive, pre-emptive and punitive self-defence. The individual has to accept that the State's use of force is legitimate *vis-à-vis* himself and that he is no longer authorized to unilaterally protect his vital interests of life, liberty and property *vis-à-vis* other individuals. However, the State, mindful of the fact that it cannot create effective deterrence against aggression everywhere, all the time, leaves part of the natural right to act in self-preservation in the hands of the individual. It is the remainder of this natural right to act in self-preservation which we commonly refer to as the right to self-defence and it includes the normative restrains of necessity, proportionality and immediacy. However, these normative restraints remain conditional upon the degree to which the State can create effectiveness deterrence against transgressors of the agreements on the mutual right to self-determination and the prohibition on the use of force against life, liberty and property. Effective deterrence to threats against life, liberty and property is to be created by either the State or by the individual. If it is not by the one, then it is by the other.

In Section 3.5, I have explained how the laws of States, naturally and logically lead to the laws of the international order. As individual States become tasked with securing the *tranquilitas ordinis* domestically, they must also secure this domestic *tranquilitas ordinis* in the sphere of international relations. The State therefore has an inherent right and duty to use force in acts of self-preservation, analogous to the way that individuals have this right in the state of nature. Because the State has inherited these rights from the individuals living in the State, the interests which the State has a right to protect are the national, collective variants of life, liberty and property, namely, respectively, sovereign existence, political independence and territorial integrity. Additionally, similar to the way that individuals have contracted out parts of their right to act in self-preservation through the use of force to protect their life, liberty and property

to their respective States, so too have States done so in the international legal order. Throughout the 20th century States have contracted out parts of their inherent right to use force in acts of self-preservation through the use of force to protect their sovereign existence, political independence and territorial integrity to the UN Security Council. However, just as is the case with domestic law systems, this transfer of power remains (to some degree) conditional upon the willingness and ability of the UN Security Council to protect States' interests of sovereign existence, political independence and territorial integrity. Effective deterrence to threats against sovereign existence, political independence and territorial integrity is to be created by either the State or by the individual. If it is not by the one, then it is by the other.

Throughout this chapter, I have tried to argue that many parts of the systems of social organization through which we try to regulate actions of the members of our national and international societies, are in fact natural. That is, they are ultimately derived from our human biological nature. I posit therefore that it is possible to draw a line of logical, natural steps from the human nature with which we are all born to the UN Security Council Chamber in New York City at 760 United Nations Plaza, Manhattan, New York City, United States of America.

In the next chapters, I will apply these findings to the domain of cyberspace. I will argue that the story of our natural steps is not finished here, at the level of the international legal order, in this chapter. Rather, our story continues in the information age with new interpretations of what it means to protect people's lives, liberty and property, as well as their collective variants of sovereign existence, political independence and territorial integrity.

In Chapters 5 and 6, I will deal with these questions specifically. In Chapter 5 I will argue that the concept of territorial integrity needs to be broadened to not just include physical space, but also that it must include the protection of the parts of cyberspace with which one makes a living in the Information Age. The protection of intellectual property - such as technologies, techniques – needs to be included in the definition of territorial integrity pursuant to article 2(4) UN Charter and large-scale theft of intellectual property needs to be defended against with claims of sovereigty. In Chapter 6, I will argue that technology is a *condition sine qua non* for Mankind to survive. I will use an anatomy analogy to argue that critical infrastructures of energy, matter and information are to the State body what the lungs, arteries and brain are to the human body. Durable disruption of these critical infrastructures thus are therefore threats to the sovereign existence of a State as well.

The next chapter, Chapter 4, will first deal with effective control over cyberspace. It will address the so-called attribution problem in cyberspace and argue that, contrary to the high seas, effective control can in fact be exercised by States over cyberspace.

I'll leave this chapter with another quote from *The Law of the Jungle* by Rudyard Kipling:

"Now these are the Laws of the Jungle, and many and mighty are they; But the head and the hoof of the Law and the haunch and the hump is — Obey!"[242]

[242] R. Kipling, The Jungle Book (1894), The Law of the Jungle.

PART III: APPLICATION

24 *Eye for eye,*

tooth for tooth,

hand for hand,

foot for foot,

25 *Burning for burning,*

wound for wound,

stripe for stripe.[243]

[243] The Holy Bible, King James Version, Exodus, Chapter 21, verses 24-25.

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.

5 Large-Scale Theft of Intellectual Property as Aggrandizement of Cyber Territory

"Shylock: *No, go ahead and take my life. Don't pardon that. You take my house away when you take the money I need for upkeep. You take my life when you take away my means of making a living.*"[385]

5.1 Introduction

In William Shakespeare's *The Merchant of Venice* Bassanio, three parties agree to a contract. Bassanio, a Venetian noble man, seeks to loan a sum of 3000 ducats to invest in a shipping expedition, after having previously already squandered his estate. He approaches his friend, Antonio, a Venetian merchant, for the loan. Although Antonio is willing to provide the loan to Bassanio, he is unable to do so because his ships and merchandise are out at sea at the time. However, Antonio agrees to act as the loan's guarantor for when Bassanio can find another lender. This lender is eventually found in Shylock, a Venetian Jew and money-lender. Shylock agrees to lend Bassanio, an outspoken anti-Semite who has previously antagonized Shylock, the sum, under the condition that, as an insurance to the loan, should Bassanio fail to repay the loan at a specified date, Shylock may then exact a 'pound of flesh' from Antonio, literally. After deliberation, Bassanio and Antonio agree to the terms as set out by Shylock and the contract is signed.

Unfortunately, this time as well, luck is not on Bassanio's side and this expedition too fails. The story progresses with a default on the payment and with Shylock taking Antonio to court to exact his 'pound of flesh'. After some discussion, Shylock is initially allowed to exact his pound of flesh as per the agreement. Soon thereafter however, the judge declares that although Shylock may take the pound of flesh, he may not take a gram more or less, lest Shylock be locked up. Additionally, Shylock may also not take the blood of Antonio as this is considered by the judge not to be included in the agreement. Moreover, the judge also declares that Shylock is in violation of another Venetian law, namely the law that holds that if a foreign resident -

[385] W. Shakespeare, The Merchant of Venice (Modern translation), *available at*: http://nfs.sparknotes.com/merchant, Act 4, Scene 1, Page 16, lines 355-369.

such as Jews like Shylock, who live in Venice's Jewish ghetto[386] and not in Venice proper – make a direct or indirect attempt to kill any citizen of Venice, that the person he tried to kill may take half of this foreigner's property, with the other half going to the state.[387] Further, this law stipulates that Shylock's life is now to be decided by the Duke.[388] The Duke, after some deliberation, decides to spare the life of Shylock and to forfeit the half of Shylock's property which is to go to the state. The other half is still to go to Antonio. Shylock, perhaps initially surprising to many, rejects the offer.

The predicament of Shylock is dire and, perhaps surprisingly, uniquely suitable to illustrate the overarching goal of this chapter, namely the importance of protecting intellectual property in cyberspace. To Shylock, the proposed sentence did not just amount to a harsh (and arguably unjust[389]) punishment and a major financial setback. Rather, it could be argued that it continued to amount to a death sentence. As a Jew living in 16th century Italy, Shylock was not allowed to own land for farming, nor was he allowed to exercise professions or serve in government. Resultantly, with the factors of production of *land* or *labor* not available to him, the only factor of production open to Jews like Shylock was that of *capital*.[390] However, in order to make a living from capital, money-lending requires a certain amount of capital to lend

[386] The name 'ghetto' comes from the word *gheta*, which means 'snail' in the Venetian dialect of Italian. It refers to so-called snails in metallurgy, which is a byproduct of foundries that looks like a mesh of snails. The Jewish living spaces in Venice were built on the spot where the iron foundries let the snails cool off.

[387] *See* W. Shakespeare, The Merchant of Venice (Modern translation), *available at*: http://nfs.sparknotes.com/merchant, Act 4, Scene 1, Page 15, lines 338-348, "Wait a minute, Jew. The law has another hold on you. The laws of Venice state that if a foreign resident directly or indirectly attempts to kill any citizen, the person he tried to kill will receive one half of the foreigner's goods. The other half goes to the state. Whether the offending person lives or dies is up to the duke—there's no one else to appeal to. In your predicament you've earned that punishment, because you've clearly contrived indirectly—and directly too—to take the life of the defendant. So get down on your knees and beg mercy from the duke.".

[388] *See* Shakespeare, The Merchant of Venice, Act 4, Scene 1, Page 15, lines 338-348.

[389] *See* Shakespeare, The Merchant of Venice, Act 3, Scene 1, Page 3, lines: "Doesn't a Jew have eyes? Doesn't a Jew have hands, bodily organs, a human shape, five senses, feelings, and passions? Doesn't a Jew eat the same food, get hurt with the same weapons, get sick with the same diseases, get healed by the same medicine, and warm up in summer and cool off in winter just like a Christian? If you prick us with a pin, don't we bleed? If you tickle us, don't we laugh? If you poison us, don't we die? And if you treat us badly, won't we try to get revenge? If we're like you in everything else, we'll resemble you in that respect." Contrary to modern legal systems, the Venetian legal system had different (sets of) rules for the different peoples living under its sovereignty. The rule which has been applied to punish Shylock could not be applied to the other, non-Jewish residents of Venice.

[390] *See* Smith, *The Wealth of Nations*, Chapter VI. In economics, the factors of production refer to the different types of inputs which, taken together, create an economic output, such as a product or service. It is this output which translates to economic value one can monetize to make a living from. In the classic definition, the factors of production are defined mutually exclusive and collectively exhaustive as land, labor and capital. Land refers to natural resources like water, air and soil, as well as the natural resources above and below them. Labor refers to the manual and mental efforts one undertakes to extract natural resources, process them [designs]. Capital refers to the technology and other goods (such as buildings, infrastructure and intellectual property) used for the production of goods and services. In more modern definitions, entrepreneurship and human capital are sometimes separated from their overarching category of labor and technology is sometimes separated from its overarching category of capital.

out to charge interest on. If half of Shylock's capital would be taken away, then, according to Shylock, he would not be able to continue (making a) living. In the eyes of Shylock, the choice between death and surrender of the means by which to make a living thus amounted to a false choice. Shylock thus replied with the words: "*No, go ahead and take my life. Don't pardon that. You take my house away when you take the money I need for upkeep. You take my life when you take away my means of making a living.*".[391]

This chapter will argue, pursuant to the legal and moral philosophy behind the principles of State sovereignty, that in the Information Age, as described in Chapter 2, our economic activity is very comparable to that of Shylock in the 16th century and that as a consequence, cyber operations which engage in large-scale, state-sponsored theft of intellectual property should be understood as territorial aggrandizement of cyber territory, analogous to physical territorial aggrandizement through large-scale, state-sponsored attacks using traditional kinetic means (*e.g.*, artillery shelling, naval attacks, aerial strikes, *et cetera*).

As explained in Chapter 3, State sovereignty is ultimately derived from the inherent drive of people to self-determination and the protection thereto by the State of the vital interests of individuals, namely; life, liberty and property, as well as their collective forms in the shape of state sovereignty, political independence and territorial integrity. This chapter and Chapter 6 deal with the inverse of State sovereignty, namely breaches to self-determination. Chapter 6 deals with threats to cyber *services* such as through the durable disruption of critical infrastructures. This chapter will continue to deal with threats to cyber *products* such as through the large-scale theft of intellectual property.

This chapter contains three main sections, dealing with, subsequently, *res nullius*, *terra nullius* and *data nullius.*

Section 5.2 will deal with *res nullius*. In this section, the legal and moral foundation for the concept of property will be set out in general and specifically, the legal and moral foundation of ownership over *physical objects.* It is argued here that ultimately, all property rights are derived from the addition of value by a person (or through the proxy of a legal entity) to natural resources which previously had the status of *res nullius*. Section 5.3 deals with *terra nullius.* This section will deal with *land* and how the cultivation of *terra nullius* establishes ownership over it. This section also addresses Rousseau's objections to property rights in general and

[391] *See* Shakespeare, The Merchant of Venice, Act 4, Scene 1, Page 16, lines 355-369

specifically, those objections to property rights over land. Section 5.4 will deal with *data nullius*. In this section, it is discussed why, from a moral and legal perspective, people can own not just land and physical objects, but also ideas when these ideas have previously been, what I call, '*data nullius*'. In this section, the differences and similarities will be discussed between gaining ownership through manual labor (objects and lands) and mental labor (ideas). In this section, it is also argued that protecting *intellectual* property is the pre-requisite to being able to 'make a living' in the Information Age.

Throughout this chapter, a legal and moral theory for the information age on property rights is built from the ground up. This theory starts with the state of nature and how in the state of nature, social animals, including humans, own their labor. From there it will be discussed how this labor can be used to provide services to other members of the group in exchange for social currency, which can be cashed in on in exchange for other services. Subsequently, we leave (most of) the rest of the animal kingdom behind us, as we discuss how *Homo sapiens* attains ownership over *physical objects* by mixing his labor with the natural resources in his surroundings. Thereafter, we will discuss how, through the mixture of his labor with land, *Homo sapiens* can attain ownership over *land*. Finally, we will discuss how ownership over *ideas* is established. By doing so, this section will bring our discussion on property and territorial integrity into the Information Age. The chapter will conclude in Section 5.5 where a summary and concluding observations are provided.

5.2 From *Res Nullius* to Ownership over Physical Objects

As set out in Section 3.3, I believe that the pervasive recognition of the right to property in political philosophy as well as in regional and international legal systems across time and space is not a historical coincidence, but rather, that it reflects a fundamental logic to legal systems which is demonstrated by both philosophy and theory, as well as by law and practice.[392] This logic is that the right to property is derived from our human nature and from our inherent drive to self-determination.

[392] *See* Section 3.2; *see also* J. Locke, Second Treatise of Government, sect. 25: "Whether we consider natural reason, which tells us, that men, being once born, have a right to their preservation, and consequently to *meat and drink, and such other things as nature affords for their subsistence.*". (emphasis added); *see also* Rousseau, On the Inequality among Mankind, part II: "Man's first feeling was that of his own existence, and *his first care that of selfpreservation.*" (emphasis added)

Understanding that the right to property is a pre-requisite to Man's self-determination, does however not explain where and when this right originates. I believe therefore that any discussion on property rights – both individual, private property rights, as well as collective, public property rights – requires one to start at the beginning, with the state of nature.

Originally, when Man was a hunter/gatherer wandering around the plains of Africa, adapting to his surroundings, he was more alike than unlike the other animals. Man was just another primate roaming around, looking for food and fending off others through the threat or the use of pre-emptive, preventive and punitive force.[393] The trees and the animals in his surroundings did not belong to him, yet.[394] Instead, the concept of ownership over property in the state of nature was either completely absent or it was limited to the duration during which one could hold some piece of fruit or meat in his hand and successfully fight others off from taking it from him. Man lived in the moment. Food did not spoil.

Man did own one thing and from this, ultimately, all ownership originates; his *labor*.[395]

Among social animals, it is understood that members of a group have ownership over their labor. Given that nearly all social animals do not build *products*, in order to understand this concept in the animal kingdom, we need to look at the *services* which they provide to the other members of their respective groups. Among social animals, there is a basic, implicit understanding that the services which the members of these groups provide to each other – such as grooming, protection and prostitution[396] - are *owned* by the providers of these services. One notably example which is very illustrative of the understanding of ownership among social animals was in a 2005 Yale study on the behavior of capuchin monkeys.[397] In the study a group of researchers taught a group of capuchin monkeys how to use money to pay for food.[398] Subsequently, the monkeys were given a certain budget to spend how they wished, such as on

---

[393] *See supra* Section 3.2.
[394] *See* Locke, *Second Treatise of Government*, Chapter 5, section 26: "God, who hath given the world to men in common, hath also given them reason to make use of it to the best advantage of life, and convenience. The earth, and all that is therein, is given to men for the support and comfort of their being. And tho' all the fruits it naturally produces, and beasts it feeds, belong to mankind in common, as they are produced by the spontaneous hand of nature; and *no body has originally a private dominion, exclusive of the rest of mankind*, in any of them, as they are thus in their natural state.". (emphasis added)
[395] *See* Locke, Second Treatise of Government, Chapter 5, section 27: " Though the earth, and all inferior creatures, be common to all men, yet every man has a property in his own person: this no body has any right to but himself. *The labour of his body, and the work of his hands, we may say, are properly his.*". (emphasis added)
[396] *See supra* Section 3.2. Unsurprisingly, the basic services which social animals provide to each other often are related to the twin goals of survival (protection) and reproduction (prostitution).
[397] *See* S. Dubner, S. Levitt, Monkey Business, New York Times, 5th June, 2005, *available* at: http://www.nytimes.com/2005/06/05/magazine/monkey-business.html (accessed on 31st July, 2017).
[398] *Id.*

different types and/or amounts of food.[399] The researchers wanted to find out how these primates would use their ability to use money to respond to different economic situations – such as gambling, egoism/altruism, time preference *et cetera*.[400] However, the researchers soon noticed that these monkeys were much more human than previously thought. When the monkeys learned that money held value which could be used to buy goods and services, they soon observed one male monkey using his money to pay a female monkey for sex.[401] After the exchange took place, the female monkey used the money to buy a grape.[402] In other words, when these monkeys learned the value of money, they reinvented the world's proverbial oldest profession. The researchers subsequently had to change the setup of their experiments to prevent the lab from turning into a brothel.[403]

Even when the understanding of ownership over services is not as explicit as in this example – with money as a medium of exchange - we can observe an implicit understanding of this concept throughout different species of social animals. They understand the underlying *social currency* which is transferred when services are provided. Actually, it is this very understanding which is the pre-requisite to allow their lives to become social. The services which social animals provide to each other in exchange for social currency can be cashed in on in different ways, even without physical currency as an intermediary. The services can be exchanged in an immediate *quid pro quo* fashion. For example, one monkey might groom another monkey and after completing the service, turn around, point at his back, and expect the service to be reciprocated right then and there. Alternatively, a monkey may deliberately groom another monkey who is higher up the social ladder without expecting to be groomed in return, but in order to acquire political capital which can be cashed in on at a later date. Brains evolve to keep score.

Certainly, there is risk involved in providing a service in exchange for social currency rather than for a physical store of value such as money (or in exchange for a physical product). The latter category can be cashed in on with much greater certainty than the former. All that is required is to keep the money (or product) until it is exchanged. However, even though no social animal besides *Homo sapiens* exchanges physical products (and until recently, money),[404] it

[399] *Id.*
[400] *Id.*
[401] *Id.*
[402] *Id.*
[403] *Id.*
[404] *See* A. Smith, *An Inquiry into the Nature and Causes of the Wealth of Nations* (1776) (hereinafter: "The Wealth of Nations), Chapter II: "*Nobody ever saw a dog make a fair and deliberate exchange of one bone for another with*

can still be expected that even in the absence of the medium of exchange of the Yale experiment, that there exists ownership over the social currency which social animals exchange through their services to each other. Although we have yet to find a way to communicate with animals with sufficient complexity to get such answers directly verbalized, there are many clues. Besides situations such as those described in the previous paragraph (of which there are many), perhaps the strongest clue that social animals keep a social currency score with the fellow members of their respective groups, is the so-called 'Dunbar's number'.[405] The primatologist Robin Dunbar discovered that there exists a strong correlation among different primate species between the size of their respective neo-cortexes and the size of their social groups.[406] Given that primate brains have a shared evolutionary history, it is believed that the reason for this strong correlation is that the size of the neo-cortex of a particular primate species provides a functional, cognitive limit to the amount of relationships they can maintain.[407] In other words, primate groups can maintain social cohesion only so far and so long as the members of the group can keep track of the relations and the social currency scores they have with the other members of the group.[408] When the amount of social relations within a group increases beyond this functional, cognitive limit, social cohesion within these groups breaks down as relations cannot be maintained and the groups themselves, break apart.

Gradually, but steadily, one such social animal in particular, *Homo sapiens*, attained ownership not just over his labor and the services he provides to the other members of his group with this labor, but also over much of his physical surroundings as well. He did this through the mixture of his labor with the natural resources in his surroundings.[409] The factor of production

---

another dog. Nobody ever saw one animal, by its gestures and natural cries signify to another, this is mine, that yours; I am willing to give this for that. When an animal wants to obtain something either of a man, or of another animal, it has no other means of persuasion, but to gain the favour of those whose service it requires. A puppy fawns upon its dam, and a spaniel endeavours, by a thousand attractions, to engage the attention of its master who is at dinner, when it wants to be fed by him.". (emphasis added)

[405] *See generally* M. Gladwell, *The Tipping Point* (2000), p. 169-192.

[406] *Id.*

[407] *Id.*

[408] *See generally* Gladwell, *The Tipping Point*, p. 169-192. The Dunbar number for *Homo sapiens* which corresponds to the size of our average neo-cortex would predict our average group size to be between 100-200 members. This number corresponds to the history of *Homo sapiens* during the times when we lived in a band society.

[409] *See* Locke, *Second Treatise of Government*, Chapter 4, section 28: "He that is nourished by the acorns he picked up under an oak, or the apples he gathered from the trees in the wood, has certainly appropriated them to himself. No body can deny but the nourishment is his. *I ask then, when did they begin to be his? when he digested? or when he eat? or when he boiled? or when he brought them home? or when he picked them up?* and it is plain, if the first gathering made them not his, nothing else could. That labour put a distinction between them and common: that added something to them more than nature, the common mother of all, had done; and so they became his private right." (emphasis added)

of *labor* became mixed with the factor of production of *land* and the *physical objects* which resulted from this mixture is his *property*.[410]

Thoughtful people can disagree on the exact *moment* when Man started owning (parts of) his surroundings, but most will agree that the *method* by which Man originally started owning (parts of) his surroundings was through a mixture of his labor with the natural resources in his surroundings.[411] Some may argue that all that is required for ownership to be established over a *physical object* is to climb a certain tree and to pluck its fruits, or to dig the earth to unearth a vegetable or to track, chase, catch and kill an animal, in order for ownership to come into being over that specific piece of fruit, vegetable or piece of meat.[412] This view reminds us of a line in the poem in *The Jungle Book* which was used to introduce Chapter 3: "*The Kill of the Wolf is the meat of the Wolf. He may do what he will; But, till he has given permission, the Pack may not eat of that Kill.*".[413] If one extracts a natural resource from nature, then, according to this view, it is extracted from the public into the private domain. This view would entail that ownership over physical objects is not an exclusively human affair, but that it exists among non-human animals as well. Indeed, among many social animals theft of gathered or hunted food evokes defensive behavior of the kind that would suggest a rudimentary understanding of the concept of ownership over physical objects. Others may argue that ownership only originates over produced *products.* That is, ownership only originates when some kind of

---

[410] *See* Locke, *Second Treatise of Government*, Chapter 5, section 28.

[411] *See* Locke, *Second Treatise of Government*, Chapter 5, section 27: "It being by him removed from the common state nature hath placed it in, *it hath by this labour something annexed to it, that excludes the common right of other men*: for this labour being the unquestionable property of the labourer, no man but he can have a right to what that is once joined to, at least where there is enough, and as good, left in common for others.". (emphasis added)

[412] *See* Locke, *Second Treatise of Government* Chapter 5, section 27: "*Whatsoever then he removes out of the state that nature hath provided*, and left it in, he hath mixed his labour with, and joined to it something that is his own, and thereby makes it his property. *It being by him removed from the common state nature hath placed it in*, it hath by this labour something annexed to it, that excludes the common right of other men: for this labour being the unquestionable property of the labourer, no man but he can have a right to what that is once joined to, at least where there is enough, and as good, left in common for others." (emphasis added); Chapter 5, section 28: "*He that is nourished by the acorns he picked up under an oak, or the apples he gathered from the trees in the wood*, has certainly appropriated them to himself. No body can deny but the nourishment is his." (emphasis added); Chapter 5, section 30: "Thus this law of reason *makes the deer that Indian's who hath killed it; it is allowed to be his goods*, who hath bestowed his labour upon it, though before it was the common right of every one. And amongst those who are counted the civilized part of mankind, who have made and multiplied positive laws to determine property, this original law of nature, for the beginning of property, in what was before common, still takes place; and by virtue thereof, *what fish any one catches in the ocean*, that great and still remaining common of mankind; or *what ambergrise any one takes up here*, is by the labour that removes it out of that common state nature left it in, made his property, who takes that pains about it. And even amongst us, the hare that any one is hunting, is thought his who pursues her during the chase: for being a beast that is still looked upon as common, and no man's private possession; whoever has employed so much labour about any of that kind, as to find and pursue her, has thereby removed her from the state of nature, wherein she was common, and hath begun a property." (emphasis added)

[413] R. Kipling, The Jungle Book, The Law of the Jungle.

additional, original value has been created or produced, such as through the taming, breeding and raising of wild animals in pastoralist societies or through the domestication, breeding, sowing, growing and reaping of fruits, vegetables and grains in agricultural societies.[414] In other words, some may argue that *capture* or *extraction* of natural resources from their surroundings is sufficient labor and mixture of labor with land to originate ownership over a physical object,[415] whereas others will argue that only *creation* or *production* based on natural resources is sufficient labor to originate ownership over a product.[416] Whether one accepts the former view of the (literal) fruits of one's labor or the latter view that one must adapts one's surroundings rather than *vice versa*, the disagreement is a disagreement of *degree*, not a disagreement of *kind*. Hence, what thoughtful people do not disagree on is the principle that the greater the relative value of the labor compared to the value of the overall object and its constituent natural resources, the stronger the claim of ownership of the laborer will be. We see this exemplified clearly when someone plucks from a tree which someone else has planted and grown. In this case, the claim of the grower is considered to be stronger than that of the plucker, as the labor of the grower has been decidedly greater than that of the plucker. Hence, the plucker may not take this particular piece of fruit without the explicit or implicit permission of the grower and the grower may ward him off until such permission is given.

We can assume that the recognition of the principle that the right to property over physical objects originates from a sufficient degree of admixture of one's labor with natural resources in one's surroundings, reflects historical reality dating all the way back to early hunter/gatherer societies. Although it might seem likely that in primitive society moral and legal ownership over property would have held little protection, as there is no police or court system in such a situation upon whom one can call, in fact, at second consideration, a more likely scenario seems to be that ownership did in fact provide sufficient protection to convince people to keep laboring for the production of physical objects. For example, even though a strong man

---

[414] *See* Locke, *Second Treatise of Government*, Chapter 5, section 32: "But the chief matter of property being now not the fruits of the earth, and the beasts that subsist on it, but the earth itself; as that which takes in and carries with it all the rest; *I think it is plain, that property in that too is acquired as the former. As much land as a man tills, plants, improves, cultivates, and can use the product of, so much is his property.* He by his labour does, as it were, inclose it from the common. Nor will it invalidate his right, to say every body else has an equal title to it; and therefore he cannot appropriate, he cannot inclose, without the consent of all his fellow-commoners, all mankind. *God, when he gave the world in common to all mankind, commanded man also to labour*, and the penury of his condition required it of him. God and his reason commanded him to subdue the earth, i.e. improve it for the benefit of life, and therein lay out something upon it that was his own, his labour. He that in obedience to this command of God, subdued, tilled and sowed any part of it, thereby annexed to it something that was his property, which another had no title to, nor could without injury take from him." (emphasis added)

[415] *See* Locke, *Second Treatise of Government* Chapter 5, section 27-30.

[416] *See* Locke, *Second Treatise of Government* Chapter 5, section 32.

could simply take the (literal or figurative) fruits of another man's labor through the use or the threat to use force if this latter man is physically weaker, it would seem likely that the stronger the claim to ownership of the weaker man pursuant to the principle discussed in the previous paragraphs, that there would be a correspondingly strong rejection by the other members of the group of this act and a corresponding political cost for the actor. Imagine the situation in a primitive hunter/gatherer society when a young man has just finished constructing a new spear. He has spent countless hours finding the perfect branch, sharpening and hardening its sharp end in fire and he has even customized it with the image of a honey badger, with which he identifies. The village has seen him toiling and working for days and knows that he is probably soon going out to try to kill a lion, a rite of passage which will earn him the right to choose a wife. Now along comes the alpha male of the group, in the prime of his physical strength, who takes the spear from him by force. Moreover, not only does the alpha male take the spear from him, but he also whacks him over the head with the back of it, turning the newly produced spear against its very creator. It would seem that the young man would have to retreat, lick his wounds and await his time, possibly when the alpha male starts showing some gray hairs. However, it seems more likely that group members of evolutionary successful groups would have – either explicitly or implicitly - recognized that the survival- and reproductive success of their group depends upon every member of the group being able to generally enjoy the fruits of their own labor.[417] Moreover, if the young man could not enjoy the fruits of his own labor, then this would also set a disturbing precedent for their own labors. Labor could quickly turn into a cheap commodity for all the members of the group. It is not unlikely that groups within early hunter/gatherer society, just as with other primates, would try to maintain social cohesion by keeping track of such transgressions against property rights by mentally subtracting an amount of social currency from their scoreboard of the alpha male and that they would eventually band up together in revolt if the situation becomes untenable and the social currency score becomes too low.[418] In other words, ownership in early hunter/gatherer societies did not just exist over labor, services and physical objects which have been extracted from their surroundings, but it likely also and especially existed over *products*. Groups which established and enforced rules around ownership over products would collectively enjoy the fruits of more such labors and

[417] *See e.g.* F. de Waal, *Chimpanzee Politics: Power and Sex Among Apes* (2007) (hereinafter: "Chimpanzee Politics"), p. 137-150. De Waal observed that among Chimpanzees within individuals there is both a lust for power and the use of force (he opened his book with a quote from Hobbes: "*I put for the general inclination of all mankind, a perpetual and restless desire of power after power, that ceaseth only in death*.") and also that for the group itself, there are dynamics which point towards peaceful behavior towards next of kin and kind.
[418] *See* De Waal, *Chimpanzee Politics*, p. 137-150.

laborers and would consequently enjoy greater survival- and reproductive success through special products for hunting, fishing, gathering and cooking. Nature selected in favor of those groups which did establish and enforce property rights and against those groups who did not. Actually, if groups of *Homo sapiens* had not established property rights, then the chance that you would be reading what I have been writing about this topic would approximate absolute zero – as a species, we would have never moved beyond producing a basic spear.

Ultimately, all property can be traced back historically to the mixture of labor with natural resources - all property started out as *res nullius*, *terra nullius* or *data nullius*. (*Terra nullius* and *data nullius* will be discussed later in this chapter.) *Res nullius*, which translates to 'nobody's property', is the legal concept whereby objects which *can* be owned, but *are not* owned by anyone, either because no one has yet established ownership over them or because someone who previously had ownership over them, has lost or abandoned it. Assuming the *capture* or *extraction* criteria for establishing ownership (as this is the lowest standard to meet for ownership), this includes wild animals, but not killed or captured animals; the fruits of wild trees, but not those who are already plucked; wild flowers, but not plucked ones; wild vegetables, but not those unearthed; wild grains, but not those sliced off; random rocks laying around, but not rocks which have been transported or processed into specific products; the wood of wild trees, but not from trees who have already been felled by someone else; water in a sea, river or creek, but not water which is captured in a bucket or produced through a rain harvesting or purification system. Through legal accession, mixture, merger and amalgamation, labor and *res nullius* merged with each other into physical objects which were owned.

Subsequently, when someone attains ownership over some physical object, including its underlying natural resources, then he may do with his property as he wishes – including exchanging it for the services or for the property of others. Eventually, through voluntary exchanges – such as purchasing, bartering, betting, gifting, inheriting, legal compensation for damages or payment in kind or the running out of a statute of limitations for stolen property – all property, with its underlying natural resources, has transferred ownership to its present day owner.

In sum, this section has discussed the origins of ownership over physical objects. In the state of nature all natural resources start out as *res nullius*. They are nobody's property. Even though ownership is largely absent in the state of nature, among social animals, members of a group do have ownership over their labor. They can use this labor to perform services for other

members of their group in exchange for social currency. They can also use their labor to capture and extract natural resources from their surroundings and claim ownership over these physical objects. *Homo sapiens* is one of only a few animals who goes beyond this. He uses his labor not just to capture and extract natural resources from the surroundings, but he also manipulates and reconfigures them in ways which creates and produces additional, original value. Although thoughtful people can disagree on whether only capture and extraction - such as is found in non-human animals as well - establishes ownership or if also creation and production of additional, original value are required to establish ownership over the natural resources extracted or produced, there is little disagreement that the greater the value of the labor in relation to the natural resources, the stronger the claim to ownership will be. In the next two sections these principles will be applied not just to ownership over physical objects from *res nullius*, as discussed in this section, but also to ownership over land which was previously *terra nullius* and ownership over ideas which were previously *data nullius.*

5.3 From *Terra Nullius* to Ownership over Land

Although we have so far discussed the general principles that ownership comes from the admixture of one's labor with the natural resources in one's surroundings and that the greater the relative value of the labor compared to the value of the overall object and its constituent natural resources, the stronger the claim of ownership of the laborer will be, we have mostly discussed where ownership over specifically *physical objects* comes from. This section expands on these principles and applies them to *terra nullius* to deal with the moral and legal foundations for ownership over *land*. Section 5.4 will deal with the moral and legal foundations for ownership over *ideas.*

When we deal with ownership over land - whether private or public - we soon come across Rousseau, who, in his *Discourse on Inequality* (1755), has famously stated that:

> "*The first man who, having enclosed a piece of ground, bethought himself of saying This is mine, and found people simple enough to believe him, was the real founder of civil society. From how many crimes, wars and murders, from how many horrors and misfortunes might not any one have saved mankind, by pulling up the stakes, or filling up the ditch, and crying to his fellows, "Beware of listening to this impostor; you are*

undone if you once forget that the fruits of the earth, belong to us all, and the earth itself to nobody." [419]

He later expounded and elaborated on how to attain original ownership over land, as the right of first occupier, in his *The Social Contract* (1762) by stating that:

"In general, to establish the right of the first occupier over a plot of ground, the following conditions are necessary: first, *the land must not yet be inhabited*; secondly, *a man must occupy only the amount he needs for his subsistence*; and, in the third place, *possession must be taken, not by an empty ceremony, but by labour and cultivation*, the only sign of proprietorship that should be respected by others, in default of a legal title." [420] (emphasis added)

From Rousseau, we can distill three criteria which need to be fulfilled in order for original ownership to be established over a plot of land; 1. ownership can only be claimed over a plot of land which is not yet owned by anybody 2. ownership can only be claimed over a plot of land which is quantitatively necessary for subsistence 3. ownership can only be claimed over a plot of land which is qualitatively claimed by mixing one's labor with the land. These three criteria will be discussed in their respective order.

When it comes to the first criteria - original ownership can only be claimed over a plot of land which is not yet owned by anyone else - we hear echoes from the previous section which dealt with how to attain ownership over *res nullius*.[421] Similar to how *res nullius* refers to natural resources which belong to nobody, so it is with *terra nullius* as well - the former refers to *physical objects* whereas the latter refers to *land* which belongs to nobody. There are two parts to *terra nullius*; a private- and a public part.[422] The former refers to a wild, uncultivated

[419] *See* Rousseau, *Discourse on Inequality*, part II.
[420] *See* Rousseau, *The Social Contract*, Book I, part 9.
[421] *See supra* Section 5.2.
[422] *See* Rousseau, *The Social Contract*, Book I, part 9: "*We can imagine how the lands of individuals, where they were contiguous and came to be united, became the public territory*, and how the right of Sovereignty, extending from the subjects over the lands they held, became at once real and personal […] *It may also happen that men begin to unite one with another before they possess anything, and that, subsequently occupying a tract of country which is enough for all, they enjoy it in common, or share it out among themselves*, either equally or according to

land which is not owned by a private individual – the latter refers to a wild, uncultivated land which also does not belong to the larger public territory of a sovereign State.[423] For example, if through seismic activity a new island would be created in the middle of the Pacific Ocean which is in international waters and which hence does not belong to any sovereign State - as all land once did - then this island would be *terra nullius* both in the private- and in the public sense. If someone would venture to this island to cultivate the fertile volcanic soil and if he fulfills the other criteria for ownership over land as well (which we will discuss below), then the plot of land he has cultivated is no longer *terra nullius* in the private sense. However, the island at large is still a *terra nullius* in the public sense, given that there is no sovereign who can rightfully claim it yet. Only after a sufficient amount of cultivated plots of land on the island become united under a collective sovereign ownership, does the island at large lose its status as *terra nullius* in the public sense. Thoughtful people can disagree on the quantity and quality of cultivation which needs to take place in order to create common, public ownership among the inhabitants of the island over the island at large, but the criteria by which this is ultimately decided must, again, be the relation between the value which is created to the value which is extracted.[424]

The second criteria which needs to be fulfilled in order for someone to be able to claim original ownership over a plot of land is, according to Rousseau, that the plot of land which is claimed is quantitatively *necessary* for subsistence.[425] The essence of this criteria is its *necessity*.[426]Rousseau does not give us guidance however, as to what constitutes this necessity. He only gives guidance as to what is *un*necessary, namely, claims of ownership which are clearly disproportional.[427] For example, during the age of discovery in which Rousseau lived, it was not uncommon for Europeans who arrived on lands which were previously unknown to

a scale fixed by the Sovereign. However the acquisition be made, the right which each individual has to his own estate is always subordinate to the right which the community has over all: without this, there would be neither stability in the social tie, nor real force in the exercise of Sovereignty.". (emphasis added)

[423] *See* Rousseau, *The Social Contract*, Book I, part 9.

[424] *See generally supra* Section 5.2. The remainder of Section 5.3 will also discuss this principle.

[425] *See* Rousseau, *The Social Contract*, Book I, part 9.

[426] *See* Rousseau, *The Social Contract*, Book I, part 9: "Every man has naturally a right to everything he needs; but the positive act which makes him proprietor of one thing excludes him from everything else. *Having his share, he ought to keep to it, and can have no further right against the community.* […] How can a man or a people seize an immense territory and keep it from the rest of the world except by a punishable usurpation, since all others are being robbed, by such an act, of the place of habitation and the means of subsistence which nature gave them in common?". (emphasis added)

[427] *See* Rousseau, *The Social Contract*, Book I, part 9.

other Europeans, to plant a flag and declare it as their own, regardless of earlier inhabitants.[428] As such, when the Dutch seafarer Abel Tasman arrived at the northern seacoast of *Terra Australis* (translation: "Southern Land"), in 1644, he had little hesitation to name it *Nieuw Holland* (translation: "New Holland", today: "Australia"), despite the fact that not only did the Dutch not cultivate or settle the land, they had not even mapped the entire coastline of this 6th largest landmass in the world.[429] Taking the logic of this method of claiming ownership over land to its extreme, this would mean that the first person who moved out of Africa missed out on a great opportunity for not pointing at the Eurasian landmass and claiming it as the property of him and his offspring.[430] It is clear and understandable why Rousseau opposes such claims of blatantly disproportionate ownership.

However, excluding just the extremes does not help us understand what constitutes "*[an] amount he needs for his subsistence*".[431] In order to understand Rousseau here, it is again important to understand the historical context in which he lived. Not only did Rousseau live during the age of discovery, but it was also the time of the third agricultural revolution in Great Britain (17th-19th century), which saw an unprecedented increase in agricultural productivity, and at the outset of the first industrial revolution in Great Britain which was enabled by this increase in agricultural productivity. At the time of Rousseau nearly all people were still subsistence farmers, meaning they produced enough food to feed most of the members of their families most of the time and that possibly, sometimes, they produced a little surplus which they could exchange for some special products. It seems unlikely that Rousseau opposed this lifestyle for its disproportionate claims on property, rather than for its extreme poverty. It seems more likely that Rousseau opposed the royal claims of ownership which sovereigns made at the time, regardless of the concerns of their subjects. Indeed, throughout his chapter on real property Rousseau criticizes sovereigns for the grand claims of ownership they make over land, not only for the above mentioned claims of ownership over land which were part of the age of discovery and which were made regardless of the concerns of earlier inhabitants, but also for

[428] *See* Rousseau, *The Social Contract*, Book I, part 9: "*Is it to be enough to set foot on a plot of common ground, in order to be able to call yourself at once the master of it?* Is it to be enough that a man has the strength to expel others for a moment, in order to establish his right to prevent them from ever returning?". (emphasis added)
[429] Admittedly, neither the Netherlands nor the V.O.C. actually claimed the land as its own.
[430] *See* Rousseau, *The Social Contract*, Book I, part 9: "When Nunez Balboa, standing on the sea-shore, took possession of the South Seas and the whole of South America in the name of the crown of Castile, *was that enough to dispossess all their actual inhabitants*, and to shut out from them all the princes of the world?". (emphasis added)
[431] *See* Rousseau, *The Social Contract*, Book I, part 9.

their claims of ownership on the lands on which their own citizens lived.[432] Contrary to earlier monarchs, Rousseau observes, monarchs at the time of Rousseau were not the kings of the *peoples* over which they ruled, but rather, they were the kings of the *lands* on which the people lived over whom they ruled.[433] Also, it must be noted that the reason most subsistence farmers did not own land beyond their most basic necessity, was not due to a lack of *willingness* to cultivate more land, but because of a lack of a *capability* to do so. As we can see from subsistence farmers from large parts of the developing world in Africa, Asia and Latin America, there is only so much land one family can farm by letting a beast of burden pull a plow.

This brings us to the third criteria for establishing ownership over land; ownership can only be claimed over a plot of land which is qualitatively claimed by mixing one's labor with the land.[434] Here we hear the echoes from Locke. As explained in the previous section, the reason why mixing one's labor with natural resources creates ownership when the amount of labor stands in sufficient relation to the rest of used resources, is because additional, original value has been created. Since the new physical object– which is created by applying labor to natural resources – can no longer be separated from its original natural resources, it subsumes the value of these resources into the new property.

The same is true for ownership over land and agricultural output.[435] The fruits of a land can belong to everyone, when they are produced by nature, or they can belong to a man, when they are produced by him.[436] When he clears the land from wild growth and keeps fighting back against nature which always tries to reclaim it, when he toils and tilts the land and when he sows and fights off pests large and small, when he waters and feeds his crops so they may grow,

---

[432] *See* Rousseau, *The Social Contract*, Book I, part 9. 'Real property' comes from English common law and refers to property over immovable objects – such as land and build structures.

[433] *See* Rousseau, *The Social Contract*, Book I, part 9: "The advantage of this does not seem to have been felt by ancient monarchs, who called themselves Kings of the Persians, Scythians, or Macedonians, and seemed to regard themselves more as rulers of men than as masters of a country. *Those of the present day more cleverly call themselves Kings of France, Spain, England, etc.: thus holding the land, they are quite confident of holding the inhabitants*.". (emphasis added)

[434] *See* Rousseau, *The Social Contract*, Book I, part 9: "possession must be taken, not by an empty ceremony, but by labour and cultivation […].".

[435] *See* Locke, *Second Treatise of Government*, Chapter 5, section 40: "*Nor is it so strange, as perhaps before consideration it may appear, that the property of labour should be able to over-balance the community of land*: for it is labour indeed that puts the difference of value on every thing; and let any one consider what the difference is between an acre of land planted with tobacco or sugar, sown with wheat or barley, and an acre of the same land lying in common, without any husbandry upon it, and he will find, that the improvement of labour makes the far greater part of the value.". (emphasis added); *see also* Rousseau, *On the Inequality among Mankind*, Part II: "for what else can a man add to things which he does not originally create, so as to make them his own property? *It is the husbandman's labour alone that, giving him a title to the produce of the ground he has tilled, gives him a claim also to the land itself*, at least till harvest, and so, from year to year, a constant possession which is easily transformed into property.". (emphasis added)

[436] *Id.*

when he protects them from wildfires and hailstorms so they won't be destroyed, then he and he alone may reap the fruits of his labor and he may claim these fruits as his own, as he is their Creator.[437] Consequently, somewhere along this line of activities, his addition of value to this land will be great enough for him to ward off others from the land and to say: "this land here, this land I have built, this belongs not to all, but to me alone, now hurry along before I have the right to defend this property.".[438]

Again, it is important to reiterate and to emphasize that this is only the case when the newly created value stands in great enough proportion to the value of the natural resources which have been withdrawn from the use by others.[439] This can be the case when a little labor is added to natural resources which are abundant and which have little value by and of themselves, such as when someone takes sand and water and turns it into the cement or bricks needed to build a house. However, it is also possible to attain ownership when a lot of labor is added to natural resources which are rare and have much value by and off themselves, such as with basic diamonds when they receive a 'brilliant cut'.[440] Actually, it is only quite recently that Mankind has started treating certain commodities as sufficiently rare to make their value to the common rise to such proportions that we require much labor to attain ownership over the extraction of these resources. Previously, when gold was discovered in this or that country, people were invited to rush in and dig it out of the ground or to sift it out of a river. Similarly with ownership over land, it is only recently that we have started to treat it as a rare commodity,

---

[437] *Id.*

[438] *See* Locke, *Second Treatise of Government*, Chapter 5, section 32-33: "But the chief matter of property being now not the fruits of the earth, and the beasts that subsist on it, but the earth itself; as that which takes in and carries with it all the rest; *I think it is plain, that property in that too is acquired as the former. As much land as a man tills, plants, improves, cultivates, and can use the product of, so much is his property.* He by his labour does, as it were, inclose it from the common. Nor will it invalidate his right, to say every body else has an equal title to it; and therefore he cannot appropriate, he cannot inclose, without the consent of all his fellow-commoners, all mankind. God, when he gave the world in common to all mankind, commanded man also to labour, and the penury of his condition required it of him. *God and his reason commanded him to subdue the earth, i.e. improve it for the benefit of life, and therein lay out something upon it that was his own, his labour.* He that in obedience to this command of God, subdued, tilled and sowed any part of it, thereby annexed to it something that was his property, which another had no title to, nor could without injury take from him." (emphasis added)

[439] *See* Locke, *Second Treatise of Government*, Chapter 5, section 40: "*I think it will be but a very modest computation to say, that of the products of the earth useful to the life of man nine tenths are the effects of labour*: nay, if we will rightly estimate things as they come to our use, and cast up the several expences about them, what in them is purely owing to nature, and what to labour, we shall find, that *in most of them ninety-nine hundredths are wholly to be put on the account of labour*." (emphasis added)

[440] The value of a diamond is assessed by 4 C's; color (the rarer the color, the more valuable it is), clarity (the clearer the diamond, the more valuable it is), carat (the larger the diamond, the more valuable it is) and cut. The cut is better the more it conforms to one of six mathematically calculated proportions which maximize brilliance (how light bounces around in the stone), fire (how the stone produces colors from white light) and scintillation (how the stone sparkles when moved around). The better a diamond is cut in such a way that it maximizes brilliance, fire and scintillation, the more value has been added to it.

especially within cities. Previously, it was only in places such as the Jewish Ghetto in Venice that land was so scarce that people started building up vertically, rather than building out horizontally. Thus, for the largest part of human history, ownership over land was established simply by adding one's labor to land which was previously *terra nullius*.

5.4 From *Data Nullius* to Ownership over Ideas

Besides ownership over physical objects and land, as discussed in the previous sections, Man can also own ideas. After all, pursuant to the principle which has been set out in Section 5.2, when one adds value to natural resources and when this added value stands in sufficient proportion to the overall value, then ownership is established, including over the natural resources underlying it. In the previous sections this principle has been applied to *res nullius* and to *terra nullius* to establish ownership over physical objects and land, respectively, including over the natural resources contained in these produced products and produced land. When one uses manual labor on a stick to turn it into a spear and when one uses manual labor to turn natural land into agricultural pastures, then one attains ownership over these physical properties.

In this section, I will argue that the same is true for specific ideas on how to make better use of *res nullius* and *terra nullius*. In other words, this section deals with mental labor. As discussed in Section 5.2 fruits, vegetables, grains and animals which are captured or produced, are subsequently owned by their captor or producer (depending on the level of labor which one deems sufficient to establish ownership), because he had mixed his labor with these natural resources. One can however also domesticate and breed a specific species of fruit, vegetable, grain or animal. In such cases he does not just own the physical animals, fruits, vegetables and grains, but also their artificially selected for design. In other words, he owns not just the *objects* themselves, but also the *idea* behind them. There are several reasons for why this is the case. One is the reasoning we have seen in the previous sections; one is rewarded for mixing his manual labor with natural resources. After all, it takes an incredible amount of physical work to domesticate and breed such fruits, vegetables, grains and animals. If someone would steal such a species of fruit, vegetable, grain or animal and uses it for his own breeding purposes, then the damages to the original breeder are far greater than the damage of the loss of the single specimen. After all, he might have spent his entire life breeding this particular species. Again,

for ownership over ideas as well, it is also not clear here how much labor has to be exercised to be able to claim ownership over it. Thoughtful people can disagree.

However, it seems that ownership over intellectual property is of a different kind than ownership over physical objects or over land and that such an emphasis on manual labor is misplaced. Contrary to ownership over objects and land, determining whether someone attains ownership over an intellectual resource is not entirely determined by the amount of *manual* labor applied directly for the *manipulation* of the natural resources. Instead, ownership over ideas is attained more by the amount of *mental* labor one has undertaken over how to *combine* natural resources in a useful way. In other words, ownership over ideas deals not with the *extraction* or *manipulation* of *material*- and/or *energy* resources, but it deals with the *discovery* of *information* resources.

Consider the universe from God's perspective. The universe contains material- and energy resources and within the laws of physics, there exists a range of possible ways for these natural resources to be manipulated and combined. This range, one can imagine, is incredibly large and only a small fraction of these combinations is useful to Mankind. Within rocks exists the possibility to subtract material until one is left with flint stones which can serve the purpose of hunting, cutting, slicing, fighting or other; within certain wild animals, and plants exists the possibility to feeding and clothing us, or, if domesticated, to serve for the purpose of transporting, laboring, protecting, accompanying us or other; within land as nature left it, exists the possibility to cultivate land which can sustain entire civilizations. Within such manipulation of a single natural resource, there is however a myriad of other useful possibilities as well. Rocks, animals- and plant species can also be disassembled to serve as basic resources for the construction of tools and structures - such as needles made from bones for sowing clothes, concrete made out of stones for building bricks and wood made of trees for building the skeletons of houses.

The possibilities for manipulation depend greatly on the resources used and on the manipulation method used. Within the resources used there are certain possibilities and restrictions. For example, even though the resources *Equus quagga* (*i.e.* the zebra) and *Equus caballus* (*i.e.* the horse) seem very similar, only within the resource *Equus caballus* exists the possibility for domestication through the manipulation method of artificial selection.[441]

[441] *See* J. Diamond, *Guns, Germs and Steel* (1997). Diamond lists six features which a wild animals needs to have in order to enable domestication; 1. they cannot be picky eaters 2. they have to reach maturity fast enough to enable breeding for useful features within a human lifespan 3. they must be willing to breed in captivity, which excludes

However, access to the full range of possible manipulations of a certain resource increases when additional manipulation methods are used. For example, through artificial selection alone, the Dutch could take the root vegetable *Daucus carota* (*i.e.* the carrot) and breed it to contain a sufficient amount of beta-Carotene to turn it orange, so that they could honor the 'father of their fatherland', Willem de Zwijger (*i.e.* Willem of Orange). However, if we expand the list of manipulation tools with genetic engineering, then one could assume that the Dutch could have also turned the resource *Daucus carota* red, white and blue, to reflect the Dutch flag. In other words, the range of possibilities for the manipulation of a natural resource is dependent upon the resource used and upon the manipulation methods employed.

Additionally, on a meta-level, manipulation methods - such as artificial selection and genetic manipulation - are, by and off themselves, rare useful ideas within the full range of possibilities for the manipulation of plant- and animals species. Other such methods which are possible, but not useful, range from Lamarckism to Lysenkoism. Additionally, through the manipulation and combination of resources, we can also discover ideas through which entire new worlds of data and information resources open up to us. For example, through the manipulation of sand we have discovered how to create glass. In the temporal sense, glasses have allowed for an effective doubling of the age during which Mankind – whose eyesight decreases with age -, can continue to perform skilled work. In the spatial sense, through microscopes and telescopes, we have discovered entire new universes, small and far.

Within the laws of physics there also exists a broad range of possibilities for how natural resources cannot just be manipulated, but also *combined* with other natural resources. Some of the most significant combinations for Mankind include the combination and manipulation of a flint and kindling to create fire; a stick and stone to create a better spear; a horse and saddle to create better means of transportation and logistics; and paper and charcoal to write down letters, words and ideas. Moreover, such useful combinations can also again be combined with other useful combinations such as the saddled soldier with spear in hand or the computers we have on our desks, in our bags and in our hands. In other words, not only can natural resources be manipulated and combined with other natural resources, but they can also be combined with (other) information resources as well.

territoriality 4. they must be docile by nature (horses and cows comply with this requirement, but zebras and African or American buffalo do not) 5. they cannot have a strong tendency to panic and flee 6. they should preferably be social and conform to a social hierarchy where humans can place themselves on top.

Natural resources – such as material- and energy resources – can be manipulated and combined with each other and with (other) information resources. This enormous range of possibilities for the manipulation and combination of natural resources - such as material- and energy resources - with each other and with (other) information resources, means that statistically, if we left it to chance, we should only be coming up with bad ideas. After all, the overwhelming majority of possible combinations are entirely useless. When an inventor tries to invent a new product or service, through the scientific process of hypothesis and testing, laborious trial and error, what he does, from God's perspective, is that he tries out some of these possible combinations in order to find out which of them have some use to Mankind. He takes them out of the world of meta-physical possibility and brings them into the world of physical reality. In other words, only through labor - albeit perhaps the mental kind in the laboratory or at the office, as opposed to the manual kind at the agricultural field or in the factory - does one bring these information resources out of the natural world and bring them into the realm of Mankind. It is as if *Homo sapiens*, which translates from Latin to 'wise man', is plucking a piece of fruit from the tree of wisdom.

Henceforth, I will refer to the entire range of possibilities for the manipulation and combination of natural resources as *data*. The useful possibilities I will refer to as *information*. Its discovery or extraction from nature can be owned.

Just as with *res nullius* and *terra nullius*, this laborious process starts with a bare, raw resource. I will call this resource *data nullius*, which, insofar as I can tell, is a term of my invention. I define it analogous to *res nullius* and *terra nullius*. It is the basic resource in the world of information before it is claimed and extracted from the natural world. For example, there exists data about the amount of forests in a tree, the nutrients in an agricultural land and the migration patterns of fish, but just as with wild animals, this data only becomes useful when it is *captured* and *extracted* from the natural world and stored on a storage device – such as paper, hard disks or in the cloud. It only becomes an information resource which can be claimed and owned when it is brought under one's control.

Again, some could argue that the mere capturing of data from the natural world through sensors gives one ownership over this data and that it therefore constitutes information, analogous to the capturing of a wild animal which had previously been a res nullius.[442] Others might argue that this is still mere raw data - analogous to land and other natural resources the

[442] *See generally supra* Sections 5.2, 5.3.

way nature has left them - and that this data first needs to be processed before a claim of ownership can be made.[443] What is clear however is that the more value is added by the inventor, the stronger his claim to ownership will be. The more one discovers about the reality of the physical world, the more the discoverer can claim ownership over his discovery.[444]

Subsequently, just as with natural resources, when it is extracted from the natural world, this data or information (depending on your view) can be manipulated and combined with other information resources to extract more useful information about the way the natural world works. For example, the modern farmer can cross-reference data about the output of agricultural fields over different years with the levels of nutrients, rainfall and pests during those years. After analyzing this data, the farmer might discover how to optimize these levels through inputs such as fertilizer, water and pesticide in order to increase the yields of his fields. Ideally, this modern farmer would turn his fields into a laboratory where he constantly runs multiple experiments at the same time. Through the scientific process of hypothesis and testing, laborious trial and error, the modern farmer innovates quickly and keeps trying to discover new, more useful ways to combine his inputs to create qualitatively and quantitatively better outputs.

One analogy which is commonly used to describe this process of exploration is that of mining. In this analogy, there is a data mine, similar to mines for precious natural resources, which is being mined for a precious natural resource - such as gold, the ultimate symbol of power. For example, in a modern goldmine, there might be 3.5 grams of gold per tonne of earth on average. In order to extract the few valuable nuggets of gold, the earth needs to be laboriously extracted and processed. Analogously, the same is true for data mines. In order to find the few valuable nuggets of information, one needs to extract data from the natural world through censors or through running trial and error experiments, and subsequently process the data by replacing, modifying or deleting incomplete, incorrect, inaccurate or irrelevant parts of the data and analyze it so that we can discover useful ideas. To bring the analogy of data as a gold mine full circle, in 2000 Rob McEwan, CEO of Goldcorp Inc. set up the Goldcorp Challenge.[445] Goldcorp posted all of its data about an underperforming gold mine in Canada online and challenged the world to come up with the best ideas on where to find the next six million ounces

[443] *Id.*
[444] *Id.*
[445] *See e.g.* P. Diamandis, S. Kotler, *Abundance* (2012), p. 77-84; *see also* Open Innovation: Goldcorp Challenge, Idea Connection, 22th October, 2009 (hereinafter: "Goldcorp challenge), *available* at: https://www.ideaconnection.com/open-innovation-success/Open-Innovation-Goldcorp-Challenge-00031.html (accessed on 31st July, 2017).

of gold in this mine.[446] Ideas were submitted from all over the world.[447] The winning team was a team from Australia of mathematicians which had never visited the mine in Ontario, but simply processed the data which had been extracted and posted online by Goldcorp.[448] The result of the challenge was an estimated three billion dollar profit for the gold mining company.[449] The prize money was a negligible half a million dollars, less than the cost of most physical gold mining machines.[450] Goldcorp could have chosen to physically extract and process mountains worth of earth, but it was far more lucrative to mine mountains of data instead. Moreover, this was not a one off event. Modern day gold mining is heavily into data mining. For example, Barrick Gold Corp., the world's largest gold miner has partnered with Cisco Systems, Inc., the largest networking company in the world, to 'take gold mining into the digital era'.[451]

Besides gold mining, we see that data mining helps us discover tremendous amounts of value of Mankind. Broadly speaking, there are two main ways in which information resources add value to Mankind; they can help create more of the same or they can create something entirely new. I will discuss them in their respective order.

Information resources are probably best known for their addition of value to Mankind by helping Mankind to do more of the same with the same amount of material and energy resources. A common misconception about the economy is that it is a zero-sum game. Just as with (agricultural) land, as discussed in the previous section, the assumption is that we will run out of other natural resources as well. Besides material- and energy resources however, as discussed, it is also possible to increase the amount of functional benefit we can have from the available material- and energy resources through information resources. In other words, even if there are limits in the absolute existence of material- and energy resources – which there certainly are - information resources can often mostly compensate for this limitation. Ramez Naam describes the different ways in which information resources can compound the functional benefit we have from natural resources. He distinguishes what he refers to as substitutes, reducers and recyclers.[452] The most striking example I have come across which can help

[446] *Id.*
[447] *Id.*
[448] *Id.*
[449] *Id.*
[450] *Id.*
[451] *See e.g.*, D. Bochove, D. Bass, Barrick Turns to Cisco to Drag Gold Mining Into Digital Era, Bloomberg, 12th September, 2016, *available* at: https://www.bloomberg.com/news/articles/2016-09-12/barrick-turns-to-cisco-to-drag-dusty-gold-mines-into-digital-era (accessed on 31st July, 2017).
[452] *See generally* Naam, *The Infinite Resource*, Chapters 9-11.

illustrate the importance of information resources to increase the availability material- and energy resources, is the availability of water, the most basic resource of all biological life, in the State of Israel. When the modern State of Israel was being re-established in the late 19th century, one of the problems which was quickly realized, was the lack of natural water resources. If the Jewish nation was to re-establish itself as a State in its historical homeland after nearly two millennia of exile, then the early Zionists would have to find ways to increase the functional benefit they could have from the water resources there. In his book, *Let There Be Water* by Seth Siegel, describes how the early Zionists created water almost (and sometimes literally) out of thin air.[453] We see the reducers, recyclers and substitutes from Naam all at play here.[454] The *reducer* refers to the more efficient use of a particular resource.[455] In the case of water in Israel, this can be clearly seen with the invention there of modern drip irrigation. Drip irrigation allows for targeted irrigation of crops, as opposed to flooding or spraying entire fields, which, when compared to drip irrigation, wastes more than 90% of the water used.[456] This simple invention thus increased the amount of crops which could be grown with the same amount of water by 10x without adding a single extra drop of water.[457] The *recycler* performs a similar functional improvement. It refers to the reuse of a specific resource in a waste stream.[458] Through a myriad of inventions Israel has become the No. 1 water recycler in the world, at a rate of over 90%.[459] By comparison, the No. 2 in the world is Spain, which recycles less than 20% of its water.[460] Again, we see that through recycling, the same amount of fresh water could increase the availability of water resources by about 10x. The *substitute* refers to a resource which provides an alternative resource base to use to perform a certain function.[461] In the case of Israel and water, this one blows it out of the water, literally. Although fresh water is irreplaceable as a way to keep our bodies' and our plants' cells hydrated, here too Israel found ways to use information resources to compensate for a lack of natural resources. Through the invention of efficient desalination technology, Israel now uses the salty water of the Mediterranean Sea to create the majority of the fresh water used in its cities.[462] Moreover, Israel expects to produce 90% of its water within a decade, for again, another 10x improvement on

[453] *See generally* S. Siegel, *Let There Be Water: Israel's Solution for a Water-Starved World* (2015) (hereinafter: "Let There Be Water").
[454] *See generally* Naam, *The Infinite Resource*, Chapters 9-11.
[455] *See generally* Naam, *The Infinite Resource*, Chapter 10.
[456] *See generally* Siegel, *Let There Be Water*, p. 55-77.
[457] *Id.*
[458] *See generally* Naam, *The Infinite Resource*, Chapter 11.
[459] *See generally* Siegel, *Let There Be Water*, p. 78-99.
[460] *Id.*
[461] *See generally* Naam, *The Infinite Resource*, Chapter 9.
[462] *See generally* Siegel, *Let There Be Water*, p. 42-54.

the use of this precious resource.[463] The fresh water lakes, rivers and the underground aquifers no longer need to be tapped to satisfy fresh water demands. Moreover, although the reducer, recycler and substitute in the case of Israel's water example each create about a 10x improvement in the availability of water resources, their effects compound. In other words, in little over a century Israel has managed to provide a 1000x improvement on the availability of its fresh water needs from the same set of fresh water resources.

What is true for water resources in the case of Israel, is true for most material- and energy resources. Increasing scarcity in the absolute amount of material- and energy resources which can still be mined is offset by the increase in the information resources which help us increase the functional use we have from these physical resources at a faster rate than we deplete them. One famous example is the Simon-Ehrlich wager. During the 1960s and 1970s biologist Paul Ehrlich, became widely cited for his book *The Population Bomb* which warned that the high population growth at the time would soon cause Mankind to outgrow the carrying capacity of the planet.[464] Ehrlich advocated in favor of population control to avoid a Malthusian catastrophe. The economist Julian Simon, in his book *The Ultimate Resource* argued that this time too, Malthusian warnings would prove to be a fallacy and that information resources would compensate for material- and energy resources.[465] Simon challenged Ehrlich to put his money where his mouth is and proposed a wager of $10.000,- to Ehrlich; Ehrlich could choose a basket of raw materials and a date more than a year away, and the two would wager on whether or not inflation-adjusted prices would have increase for these commodities, as suggested by Ehrlich.[466] Ehrlich chose copper, chromium, nickel, tin and tungsten and, just to be sure, a date ten years away from the start of the wager.[467] When the payoff date came in 1990, Ehrlich had a decisive loss of the wager as the prices of all five commodities had fallen dramatically.[468] Ehrlich declined to accept a second proposed wager by Simon.[469]

Clearly, natural resources are finite, but our access and use of them, through our resourcefulness, or information resources, is far less so. Given that so far, we have managed to

[463] *Id.*
[464] *See generally* P. Ehrlich, *The Population Bomb* (1968).
[465] *See generally* J. Simon, *The Ultimate Resource* (1981).
[466] *See* Naam, *The Infinite Resource*, Chapter 2.
[467] *Id.*
[468] *See* Naam, *The Infinite Resource*, Chapter 2.
[469] *Id.*

consistently increase the functional availability of every resource faster than we have managed to deplete them, perhaps appropriately, Ramez Naam refers to ideas as the *infinite resource*.

Besides helping us do more of the same, as discussed above, information resources can also help us create entirely new products and services. For example, although the best restaurants in the world certainly use the best products and have the best equipment to prepare the products and services they sell to their customers, the greatest increase in value for these dishes and dining experiences comes from the way they put all of these together. When one visits a Michelin star restaurant, one will notice that the price of the food cannot just be explained by adding up the costs for the natural resources (ingredients, cooking gas), labor (marketing, production costs and entrepreneurship) and capital (restaurant building, décor, training of chefs). Rather, one will find that a large share of the price is made up of the cost of the creation of the recipes used (the intellectual resources). These chefs have used their extensive training and knowledge as well as a lot of scientific process of hypothesis and testing, laborious trial and error, to come up with recipes which have the right contrasts of flavors between sweet, sour, salty, bitter and umami, of a texture which has the right balance between a firm bite and soft mouthfeel and between dry-, and juiciness. Additionally, the recipe also needs to be visually appealing, containing nicely contrasting bright colors not usually found on plates – such as greens, purples and yellows. Speaking of plates, some of the more post-modern expressions of food go far beyond transportation devices for food, but have become entire experiences all onto themselves - such as with edible floating balloons made from cheese.[470] Every part of the recipe needs to be surprising and delightful. It is science. It is art. It is originally created value.

The reason one can own an information resource such as a specific recipe, is because someone has added great value to the ingredients through their combination. Perhaps aptly phrased, resourcefulness does not refer to the amount of resources accumulated, but to the ingenuity in how to use them. As Chief Economist of the World Bank, Paul Romer, has remarked; “Economic growth occurs whenever people take resources and rearrange them in ways that are more valuable.”.[471] The potential size of information resources vastly exceeds the value of natural resources. Moreover, with the upcoming internet of things and the internet of everyone, as discussed in Section 2.4, mountains of data about the natural world and about

[470] Alinea Restaurant, 1723 N Halsted St, Chicago, IL 60614, USA, 3 Michelin stars.
[471] P. Romer, Compound Rates of Growth, *available* at: http://www.econlib.org/library/Enc/EconomicGrowth.html (accessed on 31st July, 2017).

human nature can now, for the first time ever, be extracted and processed, through a scientific process of hypothesis and testing, laborious trial and error, to come to the few nuggets of valuable information resources about how the natural world works. It will allow us to combine bytes with atoms to improve everything about our physical world, such as agriculture, forestry, fishing, drilling, mining, construction, manufacturing, professional services (legal, financial, tax, accounting and business consultancy), support services (human resource management and facility management), customer relationship management (public relations, marketing, sales and customer support), healthcare services (physical- and psychological), trade and retail, logistics, energy, (information and) communications technology, media and entertainment, art and design, education, public services and leisure (hospitality and wellness).

Through the extraction, and processing of more and more information about the physical world, we will cast a nervous system over our fields, forests and fisheries, we will overlay data mines over our oil fields and mineral mines and create a cornucopia of abundance; we will construct and manufacture structures and products with robots and artificial intelligence in a way which will make our construction and factory workers look absolutely superhuman; we will correlate human nature and nurture with diseases and banish diseases which right now scare us to death; we will have experiences physical and digital which are so perfectly tuned to our human nature and personal tastes, likes and preferences that they positively amount to bringing us heaven on earth.

However, all of this is predicated on the successful protection through which we can continue to be incentivized to make a living from producing all of this intellectual property.

In the agricultural and industrial ages, we used to explore and exploit material- and energy resources. This exploration has now largely been finished. Although there will be some anecdotal examples, we are not going to find another pool the size of the natural resources we have now. Moreover, until we manage to make space mining cost/effective, we will have to make do with the natural resources on this planet only. Fortunately, for the foreseeable future, we can do so, easily. In the information age, we will explore and exploit information resources instead. We will not find more *of* the same. We will do more *with* the same and we will do altogether new things.

Concomitantly, as the economy moves from the primary and secondary sector to the tertiary sector, the political importance of protecting the economic end products of the primary

and secondary sector - which are mostly added value *res nullius* and *terra nullius* - declines.[472] As the relative share of material- and energy derived economic activity declines in favor of information based economic activity, in a way that can only be compared with the decline of agriculture in favor of industry and the service sector, then one of the most fundamental tasks of a government, protecting property, should pivot correspondingly. The task of the State should increasingly change to not just be concerned with the protection of just air-, water-, terrestrial-, and outer space - which correspond with material- and energy resources -, but especially also with the protection of the space in which information resources are being captured, processed and transmitted. As value is mostly being produced not in physical space, but in cyberspace, States will need to respond to large-scale theft of this produced value in the same way as they would traditionally respond to theft of the land where its people live and work. In other words, States should increasingly expand their definition of territorial integrity to not just include the *physical* spaces where their citizens live and work, but also to include the *non-physical* cyberspace. Only if they can effectively protect their citizens' lives and livelihoods in this new cyber territory can they maintain their *raison d'être*. Therefore, the more a State's economy moves into cyberspace and the larger the scale of the theft of intellectual property, the more severe the effects of this theft become and therefore, the more likely it is that a State will consider such theft as aggrandizement of cyber territory.

5.5 Conclusion

This chapter started with the observation that in the information age, our economic activity is moving away from the types of economic activity which correspond to the primary and secondary sector of the economy, namely land and physical labor, to the types of economic activity which corresponds to the tertiary sector, namely mental labor and capital. Resultantly, the State needs to adjust accordingly and protect the new types of property we produce if it wants to maintain its *raison d'être.*

Section 5.2 has set out the concept of property on the most basic level. It has argued that among social animals, members of a group have ownership over their own labor. Even without the exchange of products or physical currency in exchange for labor, there is the evolved understanding that social currency exchanges owner in exchange for the value created through labor. This social currency can either be cashed in on at a later date, or, alternatively, there is a

[472] *See supra* Section 2.4.

political or social cost to pay. In this section, we have also focused on one particular species of social animal; *Homo sapiens*, because unlike nearly any other animal, we have the peculiar attribute of using our labors to turn *res nullius* into finished products.

Section 5.3 applied the principles of ownership as discussed in Section 5.2 to land and has described how a moral claim of ownership over land comes into existence. Here too, we have seen that the creator of new value becomes its rightful owner, in this case by cultivating *terra nullius* into agricultural land. The fruits of such a land are not those from nature, but those from labor and as such, they are his and his alone.

Section 5.4 applied these same principles to the information age. In the information age, value is increasingly added not by extracting more materials or producing them further into higher end products, but rather, by capturing, processing and transmitting *data nullius* into information resources. We are increasingly producing value not by creating products or lands, but by discovering ideas about the way the natural world works. Making a living in the Information Age thus entails creating intellectual property by cultivating and structuring parts of the data world. In this section, we have also discussed the consequence of this shift in importance towards the creation of intellectual property as it pertains to our social organization, namely, that the State can only maintain its *raison d'être* so long as it continues to protect our property. Therefore, as our economic activity continues to move into the domain of cyberspace, the State will follow us there and will start to consider large-scale theft of our intellectual property in this space as severe as aggrandizement of its (cyber) territory.

Councillor Hamann*: Care for some company?*

Neo*: Councillor Hamann.*

Councillor Hamann*: I don't want to intrude if you prefer to be alone.*

Neo*: No, I could probably use some company.*

Councillor Hamann*: Good, so could I. It's nice tonight. Very calm. Feels like everyone's sleeping very peacefully.*

Neo*: Not everyone.*

Councillor Hamann*: I hate sleeping. I never sleep more than a few hours. I figure I slept the first 11 years of my life, now I'm making up for it. What about you?*

Neo*: I just haven't been able to sleep much.*

Councillor Hamann*: It's a good sign.*

Neo*: Of what?*

Councillor Hamann*: That you are, in fact, still human. Have you ever been to the engineering level? I love to walk there at night, it's quite amazing. Would you like to see it?*

Neo*: Sure.*

[…]

Councillor Hamann*: Almost no one comes down here, unless, of course, there's a problem. That's how it is with people - nobody cares how it works as long as it works. I like it down here. I like to be reminded this city survives because of these machines. These machines are keeping us alive, while other machines are coming to kill us. Interesting, isn't it? Power to give life, and the power to end it.*

Neo*: We have the same power.*

Councillor Hamann*: I suppose we do, but down here sometimes I think about all those people still plugged into the Matrix and when I look at these machines, I.. I can't help thinking that in a way, we are plugged into them.*

Neo*: But we control these machines, they don't control us.*

Councillor Hamann*: Of course not, how could they? The idea's pure nonsense, but... it does make one wonder just... what is control?*

Neo*: If we wanted, we could shut these machines down.*

Councillor Hamann*: Of course... that's it. You hit it! That's control, isn't it? If we wanted, we could smash them to bits. Although if we did, we'd have to consider what would happen to our lights, our heat, our air…*

Neo*: So we need machines and they need us. Is that your point, Councillor?*

Councillor Hamann*: No, no point. Old men like me don't bother with making points. There's no point.*

Neo*: Is that why there are no young men on the Council?*

Councillor Hamann*: Good point.*

Neo*: Why don't you tell me what's on your mind, Councillor?*

Councillor Hamann*: There is so much in this world that I do not understand. See that machine? It has something to do with recycling our water supply. I have absolutely no idea how it works. But I do understand the reason for it to work. I have absolutely no idea how you are able to do some of the things you do, but I believe there's a reason for that as well. I only hope we understand that reason before it's too late.*[473]

[473] The Matrix Reloaded (2003), part 3.

6 Durable Disruption of Critical Infrastructures as a Territorial Blockade

"Councillor Hamann*: Almost no one comes down here, unless, of course, there's a problem. That's how it is with people - nobody cares how it works as long as it works. I like it down here. I like to be reminded this city survives because of these machines. These machines are keeping us alive, while other machines are coming to kill us. Interesting, isn't it? Power to give life, and the power to end it."*[474]

6.1 Introduction

In the movie trilogy the Matrix, from which the opening conversation of this Chapter originates, Mankind is in war with an army of machines. In the movie it is not made clear whether it was Mankind or the Machines which torched the sky, but the result was the same; earth is deprived of the sunlight needed to grow food or to keep warm. In this permanent dark and cold world, Mankind's last stance is in Zion, a small civilization numbering a couple of thousand people near the warm core of the earth.

The movie is very illustrative and deeply philosophical about the relation between Man and Machine. As the conversation demonstrates, even the people who were fighting against the Machines, continued to be dependent upon other machines for their lighting, heating and air-conditioning. In other words, technology continued to be a *conditio sine qua non* for Mankind to survive.

This chapter will argue, pursuant to the legal and moral philosophy behind the principles of State sovereignty, that in the Information Age, as described in Chapter 2, our society is very comparable to that in the movie the Matrix and that as a consequence, cyber operations which durable disrupt our access to our technology will be regarded as severe as a blockade of our territory by traditional kinetic means, such as through large-scale, state-sponsored (threats of) force (*e.g.*, artillery shelling, naval attacks, aerial strikes, *et cetera*)..

As explained in Chapter 3, State sovereignty is ultimately derived from the inherent drive of people to self-determination and the protection thereto by the State of the vital interests

[474] The Matrix Reloaded (2003), part 3.

of individuals, namely; life, liberty and property, as well as their collective forms; state sovereignty, political independence and territorial integrity. This chapter and Chapter 5 deal with the inverse of State sovereignty, namely breaches to self-determination. Chapter 5 has dealt with threats to *products* in cyberspace such as through the large-scale theft of intellectual property. This chapter will continue to deal with threats to *services* in cyberspace such as through the durable disruption of critical infrastructures.

This chapter will contain three main sections. In Section 6.2, I will discuss the relation between Man and Machine. In this section, I will describe the process by which people moved from the state of nature to States proper and how this has changed the common life of the people living there in such a way that people began to trade and specialize the fruits of their labors. Resultantly, I will argue, people became dependent on each other and on the technologies they produced. It will be argued in this section that technology invariably develops from a nicety into a necessity and that it needs to be regarded as an extension of the human body. In Section 6.3, I will discuss how the State is also in a symbiotic relationship with technology. Pursuant to the anatomy analogy, I will argue that critical infrastructures are extensions of the State body and that the State has similarly become dependent upon continued access to these technologies for its very survival. Thereafter, Sections 6.3-6.6 will deal with, respectively the critical infrastructures of energy, matter and information and will argue that these infrastructures need to be regarded as the respiratory-, cardiovascular- and central nervous systems of the State body. In these sections it is also described how these critical infrastructures are being increasingly connected to cyberspace and that this results in an increasing reliance on cyber security. The chapter will conclude in Section 6.7 where a summary and concluding observations are provided.

6.2 Technology as an Extension of the Human Body

As individuals and bands of people move away from the zero-sum game tactics and strategies of conquest in the state of nature[475] and towards the non-zero-sum game tactics and strategies of cooperation in the laws of men,[476] contact with other people is no longer something which is mostly to be feared. As mentioned, resultantly, this greatly reduces the amount of time and energy both groups have to spend in (preparation of, waging of and recovering from) war

[475] *See generally supra* Section 3.2.3.3
[476] *See generally supra* Section 3.3.

against the other group.[477] Correspondingly, through cooperation, there can be a great increase in the amounts of time and energy both groups can spend on finding food and on reproducing.[478] The resources of time and energy can be spend much more productively through cooperation.[479] Slowly but surely, these agreements not to use force let participants to the agreement compete successfully against other groups which did not have such agreements.[480]

Additionally, as individuals and bands of people move away from a situation in which their contact with each other was mostly of a negative nature, this also opens up opportunities for positive contact as well. One band of people can take the excessive fruits of a successful hunt to another band of people and make basic trades with them – such as for different types of foods or tools.[481] Eventually, through such trade too comes specialization as different bands of hunter/gatherers focus specifically on developing techniques and technologies for hunting-, fishing- or gathering specific types of foods.[482] Subsequently, they trade the excessive fruits of their specialized labors among each other.[483] Through trade, the different bands of people achieve greater differentiation as to the quality of the products and services they can consume - through specialization, the different bands can achieve greater quantities.[484]

Through the process of specialization and trade, new professions soon explode onto the scene as well. Specialized tool builders produce special tools for hunting, fishing, gathering, cooking and for producing clothing and shelters. At some point, as the basic *physiological* needs of people are increasingly being met, professions arrive which start to cater to higher *psychological* wants as well - such as craftsmen, artists, and priests.[485] Higher value products and services are being created, such as jewelry, arts and salvation of the spirit. Life is getting better and, according to the services provided by the priestly class; eternal.

As cooperation continues to increase, people start forming larger sociopolitical groups.[486] Bands join into larger, over-arching tribes; tribes move into larger chiefdoms and

---

[477] *Id.*
[478] *Id.*
[479] *Id.*
[480] *Id.*
[481] *See generally* M. Ridley, *The Rational Optimist: How Prosperity Evolves* (2011), Chapter 2. Chapter 2 is titled "The collective brain: exchange and specialization.". Ridley describes trade (in his words "exchange") and specialization as a process through which man outsources certain skills to the 'collective brain' of the group with which he interacts. Hence, the larger the group, the larger this brain becomes.
[482] *See* Ridley, *The Rational Optimist*, p. 47-84.
[483] *Id.*
[484] *Id.*
[485] *See* Maslow, A Theory of Human Motivation.
[486] *See* E. Service, *Primitive Social Organization* (1962).

chiefdoms themselves grow into States[487] As these groups grow larger and as their cooperation grows more complex, different types of food production are enabled and *vice versa*, different types of food productions enable more complex cooperation.[488] As chiefdoms and States increase the centralization and monopolization of the legitimate use of force and societies move into the laws of States,[489] people become increasingly freed from aggression against their lives, liberty and property. Consequently, without the fear of having the fruits of one's labors stolen, people can start to feel secure to invest more time, energy and resources into long-term schemes for food production.[490] Hunter/gatherer bands slowly turn into groups which engage in more long-term food production schemes based on these same types of foods.[491] In tribes, people take the fruits, vegetables and nuts they previously gathered and grow them themselves as they practice horticulture.[492] In chiefdoms, people take the animals they previously hunted and grow them themselves as they practice pastoralism.[493] In States, people take both the *flora* and *fauna* of their surroundings and grow them on a larger scale as they practice agriculture.[494] Food is increasingly being produced, rather than extracted.

Through the twin processes of the monopolization of the use of force and the process of trade and specialization which this enables, encounters with other people become something to look forward to, rather than something to be feared. To the average person, for the first time in human history, people outside of their own small groups are becoming worth more alive than dead.

Concomitantly, with this increasing specialization and trade also comes an outsourcing of the capacity to take care of all of one's own needs. A specialized builder of tools such as a blacksmith will no longer invest the time, energy and resources to learn the techniques which are necessary to be able to hunt, fish, gather or farm and neither will specialized clothing makers, weavers, potters, jewelers, bakers, brewers or butchers, let alone priests who are employed in the spiritual world. Although these professions all provide valuable products and services to other people's lives, they also become entirely dependent upon the remaining

[487] *Id.*
[488] *Id.*
[489] *See* Section 3.4.
[490] Hobbes, Chapter XIII: "In such condition, there is no place for Industry; because the fruit thereof is uncertain; and consequently no Culture of the Earth; no Navigation, nor use of the commodities that may be imported by Sea; no commodious Building; no Instruments of moving, and removing such things as require much force; no Knowledge of the face of the Earth; no account of Time; no Arts; no Letters; no Society;".
[491] *See* E. Service, *Primitive Social Organization* (1962).
[492] *Id.*
[493] *Id.*
[494] *Id.*

hunters, fishers, gatherers and farmers to bring them even their minimum amount of calories. Concomitantly, specialized tool builders build an ever increasing amount of technological tools to keep increasing the yields of the remaining hunters, fishers, gatherers and farmers with – they build specialized spears, bows and arrows, nets, traps, shovels, plows, saddles and many other tools to improve the efficiency of these remaining hunters, fishers, gatherers and farmers. Furthermore, these technological tools continue to require maintenance, repair, replacement and improvement by these specialized tool builders. The dependency thus also often works the other way around, as these hunters, fishers, gatherers and farmers no longer invest the time, energy and resources to learn the techniques to build these tools, as they previously did. Instead, they become entirely dependent on the tool builders to keep building their technological products so that the same high level of food extraction and production can be maintained.

Resultantly, as societies become more complex and specialized, there is a slow but steady voluntary surrender by all of a specific freedom for a benefit whose value is greater than the value surrendered – just as we did when we gave up rights to preventive, pre-emptive and punitive self-defence in exchange of improved security provided by the State.[495] Producers of food surrender the freedom to be independent in their production of tools and the producers of tools surrender the freedom to be independent in their production of food. Resultantly, independency diminishes and (inter)dependency grows. Slowly but steadily, just as defensive (self-)preservation moved from the individual to the collective, so too does economic (self-)preservation move from the individual to the collective.[496]

However, it is important to not simply take this process as a *fait accompli*, but to explore for a moment whether it is in the interest of *all* men to surrender this independence in favour of cooperation. After all, if there are exceptions by which some men can pursue their self-interest better through economic independence and self-sufficiency, then cooperation is not in their self-interest and they will hence not wish to cooperate with others through exchange and specialization.[497] Fortunately, these exceptions do not seem to exist in any way which would warrant hesitance against taking cooperation as the goal to pursue. Although there is no unanimity in theory and philosophy about the benefits of exchange and specialization over independence and self-sufficiency in the state of nature,[498] it is the correct view. In practice,

[495] *See supra* Section 3.4.
[496] *Id.*
[497] *See also generally supra* Section 3.2.
[498] *See e.g.* Rousseau, *On the Inequality Among Mankind*, Part I: "If we strip this being, thus constituted, of all the supernatural gifts he may have received, and all the artificial faculties he can have acquired only by a long process;

although self-sufficiency does not necessarily require specialization and expertise in every aspect of economic activity, it does require *proficiency* in all of them. Even in a primitive hunter/gatherer society, one needs to know where to hunt game, when and where to pick which fruits, vegetables and nuts, where to fish, and how to construct the hunting and fishing tools required for each of these, how to dry and sow hides for clothing and how to build basic shelters.[499] In a society, (much of) this knowledge is outsourced.[500] Not only is all of in all likelihood beyond the capacity of one individual, but even *if* one could successfully attain proficiency in all of these skills, life would still be an extremely poor existence. The natural way to best pursue one's self-interest in order to achieve greater differentiation as to the *quality* of the products and services we can consume, is hence through cooperation, exchange and specialization.[501]

Moreover, even if one would be able to live independently and if one could create more of the riches of life, then there is still another important argument against this type of self-sufficiency; it would be extremely inefficient. With increasing specialization and exchange, comes increased efficiency and *quantitative* benefits through economies of scale and through investment in better techniques and technology.[502]

---

if we consider him in a world, just as he must have come from the hands of nature, we behold in him an animal weaker than some, and less agile than others; but, taking him all round, the most advantageously organized of any. *I see him satisfying his hunger at the first oak, and slaking his thirst at the first brook; finding his bed at the foodt of the tree which afforded him a repast; and, with that, all his wants supplied*.". (emphasis added)

[499] *See* Ridley, *The Rational Optimist*, p. 47-84.

[500] *Id.*

[501] *See e.g.* L. Read, I, Pencil: My Family Tree as Told to Leonard E. Read: "I, Pencil, simple though I appear to be, merit your wonder and awe, a claim I shall attempt to prove. In fact, if you can understand me—no, that's too much to ask of anyone—if you can become aware of the miraculousness which I symbolize, you can help save the freedom mankind is so unhappily losing. I have a profound lesson to teach. And I can teach this lesson better than can an automobile or an airplane or a mechanical dishwasher because—well, because I am seemingly so simple. Simple? Yet, *not a single person on the face of this earth knows how to make me*." […] "My family tree begins with what in fact is a tree, a cedar of straight grain that grows in Northern California and Oregon. Now contemplate all the saws and trucks and rope and the countless other gear used in harvesting and carting the cedar logs to the railroad siding. Think of all the persons and the numberless skills that went into their fabrication: the mining of ore, the making of steel and its refinement into saws, axes, motors; the growing of hemp and bringing it through all the stages to heavy and strong rope; the logging camps with their beds and mess halls, the cookery and the raising of all the foods. Why, untold thousands of persons had a hand in every cup of coffee the loggers drink!". (emphasis added) The essay continues with the miraculous journey of the lead, the graphite, metal and the complex lacquer which coats the cedar, coming from all around the world and involving millions of people in their production. All of this to illustrate that even the most basic of riches – a simple pencil to write down ideas with – involves trade and technology on a scale unfathomable to any single human being, yet requiring all of the people and technology involved. Moreover, what is true for the simple pencil is true for every item produced (and yes, the paper you are currently reading this sentence on is a true miracle of trade and technology as well, let alone the miraculousness if you choose to read this on a computer screen).

[502] *See e.g.* Smith, The Wealth of Nations, Book I, Chapter I: "I have seen a small manufactory of this kind, where ten men only were employed, and where some of them consequently performed two or three distinct operations. But though they were very poor, and therefore but indifferently accommodated with the necessary machinery, they could, when they exerted themselves, make among them about twelve pounds of pins in a day. There are in a

Moreover, contrary to common perception, there is nothing unnatural about the drive towards efficiency such as through cooperation, exchange and specialization, and through technology. Rather, this drive towards efficiency is a core guiding principle of nature. As set out in Section 3.2, every life form acts according to its perceived self-interest in order to survive and to reproduce. Doing so is the *conditio sine qua non* for its continued existence and reproductive success in an environment where there is competition for scarce resources - such as food and reproductive opportunities. In the *locus classicus* of evolutionary biology, the lion hence chases the zebra and natural selection pushes both specifies towards beneficial traits such as speed and strength. However, besides the push towards *increased benefits*, natural selection also pushes species towards the other side of cost/benefit analysis: *decreased costs*. If we revisit the *locus classicus* of evolutionary biology again, we see that if the hunt was successful and the lion has consumed the zebra, then the lion will prefer not to move for days (except perhaps for reproductive pursuits). Because the lion, being the King of the Jungle, is at the top of the food chain, he can sleep like a king without falling prey to another predator. He only has to eat to survive. The reason why lions are notoriously inactive after eating is however not just digestive. Rather, it is for the same reason why not every animal has fantastic senses, strengths and smarts; all of these features incur a great cost in the amount of energy they require to grow and maintain. Great mental and physical strengths do not just provide benefits, but they also incur costs. Moreover, more often than not, the additional benefits stand in a negative cost/benefit relation to the costs. In other words, even though such features would be improvement in the sense of survival of the strongest, they are not so in the sense of a survival of the fittest. The guiding principle of evolution is to look for designs which can survive and reproduce *efficiently*. Hence, If you don't use it, you better lose it. A great example of this binary focus on either survival or reproduction is the Kiwi bird of the genus *Apteryx*, which translates to 'without wing'. The Kiwi bird is a native species of flightless birds from New Zealand and surrounding Islands which, because of New Zealand's geographical isolation, has evolved in an environment without natural predators. Resultantly, this environment de-emphasized survival mechanisms and emphasized reproduction mechanisms. The result is a five pound bird which cannot fly or

pound upwards of four thousand pins of a middling size. Those ten persons, therefore, could make among them upwards of forty-eight thousand pins in a day. Each person, therefore, making a tenth part of forty-eight thousand pins, might be considered as making four thousand eight hundred pins in a day. *But if they had all wrought separately and independently, and without any of them having been educated to this peculiar business, they certainly could not each of them have made twenty, perhaps not one pin in a day; that is, certainly, not the two hundred and fortieth, perhaps not the four thousand eight hundredth, part of what they are at present capable of performing, in consequence of a proper division and combination of their different operations*.". (emphasis added)

properly sense threats and which lays a one pound egg, one of the largest proportional to the size of any animal.

Homo sapiens too provides a very clear example of the drive in nature towards efficiency. By any comparison to the rest of the animal kingdom, we are an extremely unusual animal. As the hardware and software in our brains improved, it allowed us to wield fire, produce ever more advanced tools and to wear the skins of other animals as our clothing, instead of having to evolve the appropriate skins ourselves. Consequently, our bodies adapted. As Kelly observes:

> "We are not the same folks who marched out of Africa. Our genes have coevolved with our inventions. In the past 10,000 years alone, in fact, our genes have evolved 100 times faster than the average rate for the previous 6 million years. […] *Our teeth continue to shrink (because of cooking, our external stomach), our muscles thin out, our hair disappears.* […] We are coevolving with our technology, and so we have become deeply dependent on it. If all technology-every last knife and spear-were to be removed from this planet, our species would not last more than a few months. We are now symbiotic with technology.".[503] (emphasis added)

Mankind has long been in a symbiotic biological relationship with our technology. We can live without our technology like the lion can live without its teeth and claws. If we would take away our technology, we as a species would have a life expectancy comparable to the life expectancy of a lion without its teeth and claws. Just as the lion has adapted to a life with his teeth and claws, so too have we evolved to a life with our technology.

Moreover, our technology has kept evolving since the hunter/gatherer age and has done so at a much faster pace. As Kelly put it:

"*clothes are people's extended skin, wheels extended feet, camera and telescopes extended eyes. Our technological creations have become great extrapolations of the bodies that our genes built. In this way, we can think of technology as our extended body. During the industrial age it was easy to see the world this way. Steam-powered shovels, locomotives,*

[503] *See* Kelly, *What Technology Wants*, p. 21-42.

television, and the levers and gears of engineers were a fabulous exoskeleton that turned man into superman".[504]

Furthermore, as discussed in Section 2.4, what the industrial age did for manual labor, the information age will do for mental labor. In the same way that the industrial age created an exoskeleton as an extension of our biological bodies, so too the information age will create an exobrain.

Moreover, we also continue to adapt to our technology and become dependent upon it, if not biologically as was the case with our shrinking teeth, thinning muscles and disappearing hair, then in the social organization around our technology. In the next section I will argue that the infrastructures which we have built, are the technology that we have become dependent upon as a society. Pursuant to the domestic analogy as discussed in Section 3.5, I will argue that this technology is the extended body of the State body.

6.3 Critical Infrastructures as an Extension of the State Body

As cooperation continues to increase further, specialization deepens and trade starts to take place over longer distances and over larger groups of people. Consequently, as the physical distance between trading groups of increasingly specialized products and services increases, the functional distance between them needs to be decreased in order to enable the trade of goods and services. Within chiefdoms and States, this is often done through the public construction of infrastructures.

The Oxford Dictionary defines 'infrastructure' as "The basic physical and organizational structures and facilities (e.g. buildings, roads, power supplies) needed for the operation of a society or enterprise". In this reading, the operative word is 'operation'. It is the *operation* of a society (public sphere) or enterprise (private sphere) which is enabled by the physical structures which traffic materials, energy and information.

[504] *See* Kelly, What Technology Wants, p. 43-56. Kelly continues: "A closer look reveals the flaw in this analogy: The extended costume of animals is the result of their genes. They inherit the basic blueprints of what they make. Humans don't. The blueprint for our shells spring from our minds, which may spontaneously create something none of our ancestors ever made or even imagined. If technology is an extension of humans, it is not an extension of our genes but of our minds. Technology is therefore the extended body for ideas.". In this Chapter, Kelly argues that we should regard our technology as the 'Seventh Kingdom' of biology besides Eubacteria, Archaebacteria, Protista, Plantae, Fungi and Animalia, but consisting of memes rather than genes; *see also generally* M. McLuhan, *The Gutenberg Galaxy: The Making of Typographic Man* (1962) (hereinafter: "The Gutenberg Galaxy").

In agricultural societies, the transportation of produced agricultural goods and tools stands central.[505] Correspondingly, most infrastructures deal with the traffic of materials.[506] Raw materials such as agricultural goods are carried over constructed roads which extend the distance over which the wheels of a cart can carry goods before they break down, bridges are built over creeks, rivers and valleys to diminish the time and energy required to carry goods from point A to point B and harbors are dug out so that ships with deep hauls can be docked and (un)loaded.[507] In industrial societies, the manipulation of materials with energy stands central.[508] Correspondingly, most infrastructures deal with the traffic of energy.[509] Energy is extracted from mines, wells and springs in the form of coal, oil and gas and transported with trains, tankers and pipelines to places where their energy is directly used for the manipulation of material resources or indirectly through the turning of turbines which generate electricity which can be transported over larger distances through electrical grids.[510] In information societies, the extraction and processing of data into information resources stands central. Correspondingly, most infrastructures deal with the traffic of information. Information is extracted from the natural world through sensors, processed and transmitted through wired and wireless telecommunications.[511]

Just as the yields of hunters, fishers and farmers is increased through technology, so too is the functional capacity to trade goods and services across greater distances increased through the technology of infrastructures.

As cooperation increase further, specialization deepens further and trade soon starts to take place internationally as well. The process of specialization and trade that takes place among individuals within a State, also takes place beyond the State as people look for lower prices and greater product variety.

Concomitantly, just as people were no longer independent and self-sufficient within States when they started trading amongst each other, so too States are no longer independent and self-sufficient when they start trading across State borders. The consequence of this dependencies is that one is potentially exposed to great vulnerability - closing a State of from

[505] *See supra* Section 2.4.
[506] *Id.*
[507] *Id.*
[508] *Id.*
[509] *Id.*
[510] *Id.*
[511] *Id.*

the outside world or access to one's technology is likely to have dire consequences for said individual or State. States thus become dependent on other States for goods and services through trade and specialization analogous to the way that individuals become dependent on each other for goods and services through trade and specialization.[512]

In international law and philosophy, this is well understood. Resultantly, when one State uses force to block another State from access to the goods and services it acquires from other States, then the severity of this event is understood and this act is commonly considered an act of aggression and potentially also a *casus belli*.[513] Consequently, the State whose access to the goods and services it acquires abroad is allowed to use a proportional response to right this wrong.[514]

In practice, a blockade does not need to cover the entire border of another State in the case of a land blockade, the entire coast line in the case of a sea blockade, or the entire airspace in the case of an air blockade. Instead, a blockade can be enforced when the infrastructures of roads, sea- and airports are blocked. In other words, due to the fact that it is infrastructures through which this international trade is enabled, it is also its blockade which can disable it. It is for this reason that we often speak of certain infrastructures as being critical.

Whether a specific infrastructure is considered 'critical' would logically depend on the measure of necessity for the operation of a society or enterprise or, inversely, the severity of disruption to it.[515] Regardless of dealing with societies or enterprises, this can only be determined on a case by case basis so that all relevant dependencies can be considered. When it comes to critical infrastructures of States specifically, the same logic applies. To one State one thing will be critical, whereas to another State, other things might be critical. Unsurprisingly, what is 'critical' is defined differently in nearly every State and it is even often defined differently within specific States in different times. For example, the United States Department of Homeland Security (hereinafter: "US DHS") - pursuant to American Presidential directive PDD-63 of May 1998, which set up a national program of 'Critical Infrastructure Protection' – currently considers those infrastructures (or 'infrastructure sectors" as they term it) critical "*whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect*

[512] *See supra* Section 3.5.
[513] *See supra* Section 4.3.
[514] *Id.*
[515] *Id.*

on security, national economic security, national public health or safety, or any combination thereof.".[516] In other words, when the physical or economic health of (the citizens of) a country is threatened by disabling a specific infrastructure, then this infrastructure is deemed critical. In the most recent iteration of 2013, the US DHS lists 16 such critical infrastructure sectors, namely; Chemical, Commercial Facilities, Communications, Critical Manufacturing, Dams, Defense Industrial Base, Emergency Services, Energy, Financial Services, Food and Agriculture, Government Facilities, Healthcare and Public Health, Information Technology, Nuclear Reactors, Materials, and Waste, Transportation Systems, Water and Wastewater Systems. Similarly, the European Union has its own program for Critical Infrastructure Protection and considers those infrastructures critical which are "of the highest importance for the Community and which if disrupted or destroyed would affect two or more MS [Member States], or a single Member State if the critical infrastructure is located in another Member State. This includes transboundary effects resulting from interdependencies between interconnected infrastructures across various sectors.".[517]

In order to avoid the subjectivity inherent to the consequence based approach, as discussed in Section 4.3, for the purposes of this thesis, only those infrastructures will be deemed critical when they contribute substantially to the 'measures of civilization' of a State, as described by Ian Morris in his 2010 book *Why The West Rules - For Now*.[518] In this book Morris attempted to explain why, according to him, the West has ruled during 14 out of the last 15 millennia with regards to the level of 'development' of its civilization. Perhaps even more interesting than Morris' explanations on why this was the case,[519] Morris provided an appendix in the book on how he, perhaps daringly, attempted to quantitatively measure the level of qualitative development of different civilizations which allowed him to rank them accordingly.[520] He later expanded this measurement appendix into the 2013 companion volume

[516] US DHS, Directive PDD-63, May, 1998.
[517] COM(2006) 786, Brussels, 12 December 2006.
[518] *See* Morris, *Why the West Rules – For Now*.
[519] Morris concluded that during the previous centuries the single most important factor for determining whether a certain civilization ruled, was its geographic location. Morris argues that factors such as the concentration of cultivatable foods, the distances of different sea-routes and the availability of resources in certain regions determined the likelihood that those regions would instigate, respectively, the agricultural revolution, colonization efforts and the industrial revolution. The reason why geographical location is becoming less relevant according to Morris, closely relates to one of the central theses of this dissertation; that physical space is decreasing in importance and that digital space is taking over as the most important space.
[520] *See* Morris, *Why the West Rules – For Now*, Appendix. Note: this measurement does not include a measurement of morality, merely a measurement of, mostly economic development.

book *Measuring Civilization: How Social Development Decides the Fate of Nations*.[521] In the book, he goes through his extensive considerations for his measurements.[522] These measures have proven extremely apt at measuring civilization and useful as an inspiration for the purposes of this dissertation. Based on the UN Human Development Index, Morris discerns four factors which measure the development of a civilization.[523] I will discuss them in the order mentioned below and explain to which State infrastructures (public- or privately owned) these measures correspond. Subsequently, I will apply the expansion of cyberspace (caused by the acceleration, miniaturization and dematerialization in the capabilities of information technologies as discussed in Section 2.4) to these infrastructures in order to see how this expansion of cyberspace to these infrastructures influences the measure of civilization. Thereby, it becomes possible to properly appreciate the 'severity' when these infrastructures are disrupted by cyber operations.

Morris distinguished the following four measures of civilization:

1. The capacity within a civilization to capture and use energy;[524]
2. The capacity within a civilization to organize and urbanize;[525]
3. The capacity within a civilization to communicate,[526] and;
4. The capacity within a civilization to wage war in order to protect or expand a civilization.[527]

These measures of civilization provide the inspiration for my categorization below:

1. The infrastructures of energy;
2. The infrastructures of matter;
3. The infrastructures of information;

---

[521] *See* I. Morris, *The Measure of Civilization: How Social Development Decides the Fate of Nations* (2013) (hereinafter: "The Measure of Civilization").
[522] *See generally* Morris, *The Measure of Civilization*, p. 25-52.
[523] *See generally* Morris, *The Measure of Civilization*, p. 53-237.
[524] *See generally* Morris, *The Measure of Civilization*, p. 53-143; *see also* Morris, Why the West Rules – For now, Appendix.
[525] *See generally* Morris, *The Measure of Civilization*, p. 144-172; *see also* Morris, Why the West Rules – For now, Appendix.
[526] *See generally* Morris, *The Measure of Civilization*, p. 218-237; *see also* Morris, Why the West Rules – For now, Appendix.
[527] *See generally* Morris, *The Measure of Civilization*, p. 173-217; *see also* Morris, Why the West Rules – For now, Appendix. *See* Morris, The Measure of Civilization, p. 25-52, Section 9; *see also* I. Morris, The Measure of Civilization, Chapters 3,4,6,5 for discussions on energy, social organization, information technology and war-making capacity respectively; I. Morris, Why the West Rules – For now, Part I, Section 3; I. Morris, Why the West Rules – For now, Appendix.

4. The infrastructures of effective control.

In the sections below, I will discuss the infrastructures of energy, matter and information and justify my interpretation of Morris' classification. The 4th measure of effective control through war-making capacity has already been discussed in Chapter 4.[528]

6.4 The Infrastructures of Energy as the Respiratory System of the State

The first type of infrastructure which will be discussed is the infrastructure dealing with energy. It is defined by Morris as the full range of energy captured and used by a civilization, divided into the categories of food and fuel.[529]

Food, both plant- and animal-based, is the energy derived from food which can be consumed directly or which can be fed as feed to other animals in exchange for labor services or animal based products – such as meat, milk, wool and leather. Food as a category of energy capture is the primary means of energy capture and use in hunter-gatherer and agricultural civilizations.[530] Fuel, defined by Morris as non-food energy sources, consists of *inter alia* dung, wood, peat, coal, oil, natural gas, solar, wind, hydro, geo-thermal and nuclear power and can be used for lighting, cooking, heating, cooling, computing and powering other machines. It is the primary means of energy capture and use in industrialized civilizations.[531]

The "capacity to capture and use energy" as defined by Morris is translated in this dissertation as those infrastructures dealing with energy. In other words, it concerns those infrastructures which are responsible for the capture, transportation and use of energy. Energy is what powers civilizations and has, according to Morris, historically been the most defining measure of civilization.[532] The reason why the ability to capture and use energy is so determinative for the collective measure of civilization, is because it greatly influences the carrying capacity of the territory over which a civilization rules. Consider the following example of the fictitious *Terra Cyberia*.

---

[528] *See generally* Chapter 4; *see especially* Sections 4.2-4.3 and 4.7
[529] *See* Morris, *The Measure of Civilization*, at. 52-142. Morris also considers raw materials used for clothing and shelter to fall within the term 'energy capture', although this would technically fall under energy conservation. Since the impact of conservation is only of minimal importance according to Morris, for the sake of brevity, this will not be covered separately; s*ee also* I. Morris, *Why the West Rules – For Now*, Appendix.
[530] *See* Morris, *The Measure of Civilization*, at. 52; see especially Figure 3.1 on the Framework by Earl Cook.
[531] *See* I. Morris, *The Measure of Civilization*, p. 52.
[532] *See* Morris, *The Measure of Civilization*, p. 25-52.

Terra Cyberia is an island archipelago a 1000 kilometers west of mainland Ecuador, consisting of a group of quantitatively and qualitatively identical islands – they are identical in size and identical in all relevant other properties.

On *Terra Praedator Congregantis* people patiently spend their days gathering fruits and vegetables. The people are semi-settled, moving around the island when this or that food is in season. Occasionally, the men leave their women and children for a few days or weeks to hunt the local birds and boars that came to the island from the mainland. When they return after a successful hunt, festivities are held in their honor and the people thoroughly enjoy the meat as a delicacy. The people mostly live in the moment, eat organically and enjoy an unpolluted environment. Their largely monotonous lives are only interrupted by the occasional scarcity of food. Due to these shortages, girls on the island are older when they have their first periods and often skip menstrual cycles when their fat percentage drops below 15%. Pregnancies, when they do occur, are often naturally aborted for the same reason and when pregnancies do result in birth, both the child and the mother have a great chance of dying during or soon after birth. Infanticide is an accepted choice of contraception. If the child and/or mother do survive birth and if the child is not post-natally aborted, the rest of their lives are generally short regardless. Senicide is not unheard off. The people on *Terra Praedator Congregantis* are part of nature and life is in balance.

On *Terra Agracultura Victum* people have cut into the jungle and have replaced parts of it with agricultural lands. They spend their days producing their food by tilling the soil, sowing seeds and reaping the fruits of their labor. Food is rarely in short supply, but the elders still remember the tropical storms that once wreaked havoc on the crops. They live by the seasons, but they also try to diversify their investments in food production by engaging in long-term schemes to further domesticate more plants and animals. With each harvest, the crops give better yields and the domesticated boars are nicely fattened by the organic waste left-over from the fields. The people on *Terra Agracultura Victum* are settled near their agricultural lands and nature and man live next to each other.

On *Terra Labor Industria* it seems as if every year new mechanical contraptions are invented to which much of the heavy labor is outsourced. Water mills grind the grain into flower, wind mills seem to divert the water of entire rivers to agricultural lands and large ovens are build where wood and coal are burned to shape the local iron ore into all sorts of useful tools such as axes to clear more land, shovels to dig deeper ditches and strong wheels for carts

to bring produce from the land to the people. The people on the island not only survive; they thrive. People reproduce with great success and on this island the elders are not just extra mouths to feed, but also extra brains to store information about the way the world works. The people expand in breadth and depth on the island – they increase the productivity of their existing lands and expand further into the jungle.

As demonstrated by *Terra Cyberia*, the strategies for capturing and using energy vary greatly and so do their survival and reproductive successes. One could imagine that *Terra Praedator Congregantis* could contain a population numbering a thousand people, *Terra Agracultura Victum* 10.000 people and *Terra Labor Industria* 100.000 people, despite the islands being of identical proportions and identical properties.

Inversely, when a civilization such as *Terra Labor Industria* would lose access to its technology, its large population would collapse, fast. As historian Jared Diamond documents in *Collapse – How Societies choose to Fail or Succeed* and in *Guns, Germs and Steel: The Faith of Human Societies*, historically speaking, energy shortages through exhaustion of important resources (or through a changing climate), have been the most predictive factors in determining whether a civilization would continue to survive or whether it would start to die. It thus behooves us to briefly reflect on how our energy infrastructures expose us to potential disruptions. Our modern global civilization is powered by fossil fuels, ranging from the fertilizers used to produce the foods on our farms to the fuels used to power the machines in our factories. As Diamond warns, as a result of this reliance and dependency on fossil fuels, our modern global civilization is not immune to the threats of climate change and energy shortages. Since Mankind started using fossil fuels (coal, oil, natural gas) to power our industrial machines and fertilize our agricultural lands, the modern global civilization has exploded in the carrying capacity of our territories and in population growth. Coincidentally however, the use of fossil fuels has contributed to a changing climate, the likely results of which include extreme weather, floods, droughts, famines, wars and streams of refugees. At some point, this process of climate change needs to be slowed (and possibly even reversed) at its cause or great investments need to be made in fighting its symptoms. Additionally, even if fossil fuels did not contribute to ecological destruction or if its consequences could be dealt with in a cost-effective way, the *fossil* in fossil fuel indicates that this source of fuel is not a fuel which will last us into the future, at least not forever. It is important to understand that our modern civilization is built on the ability to withdraw energy from the fossil fuel bank, without making deposits to it, the eventual consequence of which should be clear to anyone who has ever owned

a bank account. Although it is unlikely that our modern global industrialized civilization will ever completely exhaust fossil fuels, the increasing costs to capture and use the next drop of oil or nugget of coal will, at some point, likely make fossil fuels economically unfeasible to power our civilization. Hence, at some point, sooner or later, we will either have to switch our modern global civilization to other sources of fuel, or, as other civilizations have done before us, grind to a halt and collapse.

It is important to have a proper appreciation of the gravity of this possibility. If our civilization comes to be without the fuel to power our industrial machines or fertilize our agricultural lands, then any discussions within legal theory or political science on civilization will largely be a theoretical (or even moot) exercise, because there will be no more civilization to discuss legal theory or political science for, just a much smaller world population consisting of groups of hunter-gatherers and subsistence farmers who will have been thrown back into a state of nature. Hence, in order to avoid the collapse of our modern global civilization, at some point, the increasing costs of our unsustainable energy usage - both with regards to the economical and ecological costs – means we will have to switch our energy infrastructure from fossil fuels to more sustainable sources of energy – such as solar, wind, hydro, geo-thermal and possibly, temporarily, nuclear energy as well.[533] We either go green or we will have more urgent matters to worry about than law, namely our "nasty, brutish and short lives".[534]

Making this switch to sustainable sources of energy however, will make our energy infrastructure wholly dependent upon cyber security. As detailed above, the measure of energy is divided into the categories of food and feed on the one hand and fuel on the other, the former dealing mainly with the infrastructures of the agricultural and fishing industry and the latter dealing with the infrastructures of oil, electricity and nuclear. Their connection to cyberspace will be discussed in their respective order.

The connection of the food infrastructures of agriculture and fisheries to cyberspace will only be covered briefly as it has been mentioned before.[535] In short, cheap sensors and connectivity can cast a nervous system over the means of food production to monitor and

[533] Nuclear power currently supplies between 10-15% of annual energy production and consumption, mostly in Western states such as Japan and France. Although there are no economical or technical barriers to scale this up to 100% of worldwide energy production and consumption, there are three main reasons why such adoption of nuclear energy is unlikely and/or undesirable. First, nuclear energy is unpopular due to perceived risks. Two, scaling up nuclear energy up worldwide could open up a Pandora's box of proliferation risks. Third, nuclear energy is also a non-renewable fossil fuel which will run out at some point.
[534] *See* Hobbes, *Leviathan*, Chapter XIII.
[535] *See supra* Section 2.4, 5.4.

experiment with the most resource efficient means of production. The result of this will be that agricultural farms can do much more with much less and that fish farms can provide us with great amounts of *fruit de mer*. Similar to the expansion of cyberspace, we could take the same amount of agricultural land and increase the capacity on it or we could have the same agricultural output on a smaller land. For example, The Netherlands is 134th in size, but 2nd in agricultural exports in absolute numbers.

The connection of the infrastructures of fuel is even more promising. Electrical infrastructure is currently organized as a so-called just-in-time system, which means that all of the electricity used by our lighting, cooking, heating, cooling, computers and other machines has been generated just milliseconds prior to use.[536] Balancing the tremendously complicated supply and demand of all this electricity – which needs to happen in order to prevents black- or brownouts - is already being done by connecting our energy infrastructure to cyberspace.[537] This connection of our electricity infrastructure assets to cyberspace allows utilities to analyze and predict the electricity demand and adjust the power supply accordingly - using mostly peaker gas plants and some hydro storage.[538]

In the future, this will become even more so, due to the intermittency of green energy sources.[539] Intermittency means that the output of these energy sources is not consistent due to varying intensities of wind and solar power during the days, weeks and year(s).[540] Moreover, our current centralized electricity infrastructure is based on dozens or hundreds of power plants per State.[541] A green infrastructure will be decentralized and contain millions upon millions of power plants in the form of solar panels and wind mills.[542] Basically, the electricity infrastructure will become a network, like the internet is today. Balancing this exponentially more complicated infrastructure requires intensive connection of electricity to cyberspace in order to predict electricity supply and demand based on everything from daily weather predictions which influence solar radiance and wind strength to the match schedule of the football world cup finale every four years when millions of people turn on their televisions and frying pans. With cyberspace it becomes possible to make these tremendously complicated

[536] *See generally* A. Lovins, *Reinventing Fire – Bold Business Solutions for the New Energy Era* (2011) (hereinafter: "Reinventing Fire"), p. 164-222.
[537] *Id.*
[538] *Id.*
[539] *Id.*
[540] *Id.*
[541] *Id.*
[542] *Id.*

calculations and to turn on so-called virtual power plants, demand response units and to charge and discharge electric car batteries.[543] Without cyberspace, this tremendous balancing act is simply impossible. In other words, the energy grid of the future will have to become a network for energy like the internet is a network for data. This requires tremendous amounts of data and continuous reliance on cyberspace.

With this connection of the energy infrastructure to cyberspace however, also comes a vulnerability for cyber attacks. Given the outward facing nature of our current and future energy infrastructures systems, cyber operations can potentially bring down the entire energy system. Even without causing any physical destruction, the mere functional disruption of our energy infrastructure through cyber attacks, can hence bring an entire State to its knees much quicker and much easier than traditional armies every could.

In the Hobbesian analogy of the State body, our energy infrastructures can be considered as the respiratory system in the body of the State. It provides us with the oxygen which fuels everything. Any disruption to it will therefore be as severe as suffocating. The more a State's energy infrastructures become dependent upon the well-functioning of cyberspace and the more durable the functional disruption which is caused by a cyber operation, the more severe the effects of this disruption become and therefore, the more likely it is that a State will consider such disruption as a blockade of energy from its territory.

6.5 The Infrastructures of Matter as the Cardiovascular System of the State

The second type of infrastructure which will be discussed, corresponds to the capacity within a civilization to transport goods and persons. Morris uses the size of the largest city within a civilization as a proxy to measure its level of social organization and urbanization.[544]

The reason for choosing the largest city as a proxy, is that up until the industrial revolution, the capacity within a civilization to capture and use energy had been largely fixed - the energy available to these civilizations came from the food which could be hunted, gathered or farmed.[545] It is important to understand that in hunter-gatherer and agricultural civilizations, it matters a great deal how much energy it costs to bring food from where it is hunted, gathered

[543] *Id.*
[544] *See* Morris, *The Measure of Civilization*, at. 143-171.
[545] *See* Morris, *The Measure of Civilization*, at. 143-171; *see also* Morris, *The Measure of Civilization*, at. 52-142.

or harvested, into a population center.[546] As cities grow beyond a certain size, they require increasingly more energy to transport the same amount of calories into population centers.[547] At some distance, the amount of food brought into a population center requires more energy to transport, than that it carries in calories. When this happens, a city can no longer feed itself and will collapse unto itself.[548] As explained in the previous subsection, most civilizations had already discovered, through trial and error and artificial selection and domestication of certain food species, which food sources provided the most efficient calorie per unit of volume, weight and necessary resources invested. Beyond this point, since the amount of energy which could be captured and used in a specific territory was largely fixed in hunter-gatherer and agricultural civilizations, the size of a certain city depended largely on how efficient it could transport goods and persons.[549] With a fixed ability to capture and use energy, the logistics of urbanization and transportation constitute the defining factors for city size within these earlier civilizations.

Transportation infrastructure deals with the logistics of moving around goods and persons. In other words, transportation of goods and persons deals with the infrastructure and logistics of matter. It concerns infrastructures dealing with every which physical way – such as water, land and air.

Historically speaking, the wheel, the domestication of animals, large seafaring ships and other ways of increasing the efficiency with which atoms can be moved per unit of energy, have all provided a multiplier effect on the energy captured and used.[550] Both the Islamic and Dutch golden ages owe much of their success to their respective ships – large wooden seafaring ships in the case of the Dutch and camels in the case of the Arab world (often referred to as 'ships of the desert').[551] With the industrial revolution, paved roads, rail roads and water ways took it one step further and increased the functional space of land, air and water ways exponentially. Unsurprisingly, most cities used to be based around water ways, because transportation by water is far more efficient than over roads, especially wobbly roads which easily destroy wheels and carts.[552]

[546] *See* Morris, *The Measure of Civilization,* at. 143-171.
[547] *Id.*
[548] *Id.*
[549] *Id.*
[550] *See* Morris, *The Measure of Civilization,* at. 143-171.
[551] *Id.*
[552] *Id.*

The connection of cyberspace to our transportation infrastructure has been an ongoing process in our ever-urbanizing world, but there is much room for functional growth through the connection of atoms with bits. In our modern industrialized civilization we have built cities with populations numbering in the tens of millions, whereas the largest cities in pre-industrial times numbered a mere fraction of this.[553] Perhaps even more amazingly, we have not just sprawled these cities ever wider, but we have actually managed to maintain cities with population densities of tens of thousands of people per square kilometer. In these cities, energy is no longer the problem, physical space is. The connection of transportation infrastructure to cyberspace has long been an indispensable tool to unclog the congestion in the arteries of our cities.

With the acceleration and demassification of the capacity of information technologies, cyberspace is expanding further into our transportation infrastructures. The result of this expansion will be that the transfer of goods and persons can become much more efficient with regards to the time, energy and other resources used. The three trends most important in this regard are the electrification of transportation, autonomous transportation and on-demand public transportation, all of which are entirely dependent upon cyberspace.

Electrification of transportation is an obvious necessity in order to diminish our dependence on fossil fuels, as discussed in the previous section.[554] However, transportation consumes a relatively large amount of energy and in order to make electric driving practical, batteries need to be filled quickly.[555] Switching transportation to electricity therefore requires a tremendous coordination of demand and supply in energy. Cars need to be in constant communication with the energy infrastructure so that it can be predicted when and where which cars will either charge or discharge on the net.[556] Autonomous transportation enables Mankind to take the next step after cruise control, crash prevention and auto-park and eliminates the need for human driving altogether, first just on the freeway, then on every way.[557] Not only will this free people from the task of driving and enable them to work during commutes, but it will also save hundreds of thousands of deaths caused by human driving.[558] Also, having cars think for

[553] *See* Morris, *The Measure of Civilization*, at. 143-171; *see also* Morris, Why The West Rules – For Now, Appendix.
[554] *See* Section 6.4; *see also* Lovins, Reinventing Fire, p. 14-69.
[555] *See* Lovins, Reinventing Fire, p. 14-69.
[556] *Id.*
[557] *See especially* S. Heck, M. Rogers, *Resource Revolution – How to Capture the Biggest Business Opportunity in a Century* (2014) (hereinafter: "Resource Revolution"), Chapter 3.
[558] *See* Heck, *Resource Revolution*, p. 59-100.

themselves makes it possible for them to drive very close together, almost as a train.[559] This helps reduce aerodynamic drag and frees up space on the roads so that both energy and time in transportation are reduced.[560] The effect will be a further freeing of Mankind from the limits of distance. People can start living beyond city centers as time and space experientially, functionally disappear. Additionally, autonomous driving also enables the elimination of the need for ownership of vehicles altogether. Just as music, movies and TV-series are no longer owned, autonomous driving cars also make it possible for transportation to be accessible at the press of a button.[561] When you consider that the average car is used perhaps during just 5% of its lifetime and is collecting dust and rust during the other 95% on expensive parking spaces, and when you consider that when cars are actually driving, that they tend to be occupied to only 20-25% of capacity, then it becomes clear that our transportation would benefit greatly from a switch from ownership to access at the press of a button.[562] Compared with that kind of convenience, a car that you own — which you have to park, fill up, fix, insure, clean and pay for deprecation whether you use it or not — begins to seem like kind of a drag. Goods and services are becoming on-demand or on-tap, accessible at the flip of a switch, rather than owned and stocked.

Correspondingly, as our transportation infrastructure transforms our cities, we become exposed to new disruptions to it. Whereas traditional military instruments would use explosives to destroy roads, airports and bridges, cyber operations can now, functionally, create the same amount of functional disruption to our societies at the push of a button.

In the Hobbesian analogy of the State body, our transportation infrastructure can be understood as the cardiovascular system in the body of the State. It provides us with the transportation of nutrients where they are needed. Any disruption to it can be as severe as a heart attack. The more a State's infrastructures of matter become dependent upon the well-functioning of cyberspace and the more durable the functional disruption which is caused by a cyber operation, the more severe the effects of this disruption become and therefore, the more likely it is that a State will consider such disruption as a blockade of matter from its territory.

[559] *Id.*
[560] *Id.*
[561] *Id.*
[562] *Id.*

6.6 The Infrastructures of Information as the Central Nervous System of the State

The third type of infrastructure which will be discussed, deals with the capacity within a civilization to communicate. In other words, it is the means of moving information, which more or less takes place without adding significant marginal energy or material costs for each additional bit of information. Where transportation infrastructure deals with the infrastructure and logistics of matter, and energy infrastructure deals with the infrastructure and logistics of energy, information infrastructure deal with the infrastructure and logistics of data.

From the stone tablets of Moses to the high-tech tablets of Jobs, efficient communication has greatly influenced the ability within a society for knowledge to be stored, processed and transmitted. In the case of Moses, the ten commandments, the Torah and the Talmud allowed the Jewish people to survive an exile from their historic homeland lasting two millennia without being destroyed or assimilated, a feat unequaled in recorded history. In the case of Jobs, the focus on the efficiency of communication has resulted in a user interface of home screen- and icons which has remained largely unchanged even after a decade (which translates to about two millennia in technology years).

The connection of cyberspace to our information infrastructure is of course by now a well-known phenomenon – actually, when most people think of cyberspace or the internet, the first thing they think about are our modern communication platforms. Shirky discerns five historical events in modern history, which, according to him, qualify as communications revolutions – which he defines as a moment in history when a communication technology greatly increased the expressive capacity of persons.[563] The first such revolution was the advent of the printing press, which, for the first time, allowed for one-to-many static text-based communication.[564] The second revolution was the advent of the telephone, which allowed for one-to-one real-life communication between individuals over great distances.[565] The third revolution was the advent of audio and video recorders and players, which allowed for one-to-many dynamic audio- and video-based communication.[566] The fourth revolution was the harnessing of the broadcasting spectrum, which allowed for real-time one-to-many audio and

[563] *See* C. Shirky, How the Internet will (one day) transform government, June 2012, TED 2012 *available* at: http://www.ted.com/talks/clay_shirky_how_the_internet_will_one_day_transform_government (accessed on 31st July, 2017).
[564] *Id.*
[565] *Id.*
[566] *Id.*

video-based communication.[567] The fifth and current revolution in communication is that of the internet, which allows, for the first time in history, many-to-many dynamic communication – including everyone everywhere - through text, audio and video on *inter alia* websites, -logs (web- and video based) and social platforms.[568] Moreover, as Shirky notes, the internet is more than the printing press writ large. Rather, the addition of cyberspace to our communications has, to a large degree, usurped all previous communication technologies – such as books, radio and television.[569] Information has never spread so far and wide – crossing time and space without friction. Additionally, with the continuing increase in transmission speeds, tele-conferencing and other communication technologies aimed at collaboration in the workplace, we can expect to attain virtual reality types of resolution and thus decrease the need to travel to an office building altogether (or the office building to be built in the first place).

With this connection of all of our communication infrastructures to cyberspace, our communication has become wholly dependent upon the security of our cyberspace. Moreover, any disruption to our communication infrastructure does not just influence our communication, but it also has cascading effects to our other infrastructures, including to our infrastructures dealing with energy and matter.

In the Hobbesian analogy of the State body, our information infrastructures truly are the central nervous system in the body of the State. They control and command all within the body. Disruption to it can be as severe as having a stroke. The more a State's information infrastructures become dependent upon the well-functioning of cyberspace and the more durable the functional disruption which is caused by a cyber operation, the more severe the effects of this disruption become and therefore, the more likely it is that a State will consider such disruption as a blockade of information from its territory.

6.7 Conclusion

This chapter started with the observation that Mankind is in a symbiotic relationship with Machines and that the same is true for the State; we are becoming increasingly dependent upon the well-functioning of our technology. Blocking us from our technology can therefore have

[567] *Id.*
[568] *Id.*
[569] *Id.*

severe consequences. Resultantly, the State needs to adjust accordingly and protect our access to our technology if it wants to maintain its *raison d'être*.

Section 6.2 started with the state of nature and our first contact with technology. It discussed the process by which we first acquired tools as extensions of our human bodies. Subsequently, it discussed how we gradually moved from our animal bodies to the modern cyborgs we are today and it discussed how we became dependent upon our continued access to our technology for our very survival.

Section 6.3 continued with our social organization and argued that the State has developed a symbiotic relationship with technology as well. Pursuant to the anatomy analogy, I have argue that critical infrastructures are extensions of the State's body and that the State has similarly become dependent upon continued access to these technologies for its very survival.

Sections 6.4-6.6 discussed three types of critical infrastructures of the State body, namely; the infrastructures of energy, matter and information. These sections argued why these infrastructures correspond to the respiratory-, cardiovascular and central nervous systems of the State body and these sections have discussed how these infrastructures are each becoming increasingly connected to cyberspace. Consequently, cyber operations can increasingly cause severe functional disruption to these infrastructures, thereby blocking the movement of energy, matter and information in the State body. In these sections, it has been argued why the durable disruption of these critical infrastructures through cyber operations therefore needs to be considered as severe as disruptions to the respiratory-, cardiovascular- and central nervous system of the body. Just as with the human body, these systems do not need to be destroyed to cause severe effects, durable disruption is enough. Therefore, as States become increasingly dependent upon the well-functioning of critical infrastructures and as these infrastructures become increasingly dependent upon the well-functioning of cyberspace, the State will follow us there and will start to consider disruption of these infrastructures through cyber operations as severe as a blockade of energy, matter or energy from its (cyber) territory.

PART IV: CONCLUSION

7:46 *You open your eyes. Your eyes don't hurt because your wearable has woken you up at the right time in your sleep cycle. Wearables had been going out of style for a few years, until companies started mining sleeping data for useful nuggets of information about how to nudge people into better sleeping behavior. When you learned that your particular sleep cycles are unusually disturbed by salty food, you cut back on your salt intake and have been sleeping like a baby ever since. You still sleep with a wearable to notice when work is becoming too stressful so that you know when you need make adjustments or take a vacation. You are now always connected to cyberspace.*

8:35 *You connect to work. With the advent of virtual reality, much more work can now be done from home while it is still possible to maintain a social bond with the work place (wherever that can be said to exist nowadays anyway). Many people have set up virtual reality rooms in their home offices so they can have a simulated work environment with their colleagues. It used to be expensive to do so, but then again, so was setting up a computer system at one point.*

13:52 *You get into your car. You are going to meet with a client and you want to shake the other person's hand and look them in the eye. The car is not yours. It is far too nice. As transportation network companies started using autonomous cars which pick you up within minutes of ordering, this saved a tremendous amount of costs of cars standing idly by, gathering just dust and rust. The saved costs have been added back in added luxury. A nicety invariably developed into a necessity. Your drive to the city is 50 minutes, which it usually is. You sit back and start preparing your presentation. If you would have needed to drive the car yourself, then you would have chosen to live closer to the city, but you don't have to, so you didn't choose to. As did many others. Marchetti's Constant was broken. The trend of people moving into cities was reversed and housing costs normalized. The saved costs from housing are now spend on larger houses and on housing services – such as gardeners, cleaners, cooks and personal coaches for physical, mental and spiritual health.*

14:45 *You meet your client. You are a miner, both in the traditional and in the modern sense. With the advent of autonomous driving came a quick push towards the electrification of cars. The more a car drives, the more it needs to bring down its cost per kilometer and electric driving*

was just the way to do that. The prices of several natural resources which are used to build car batteries have shot through the roof in the previous decade and your company has found a new way to correlate vegetation growth from satellite imagery with the resources needed. Business is booming.

19:15 *You connect to play. You work hard and play hard with your virtual reality headset. When virtual reality started making real progress, entertainment companies initially tried to play movies on it, just like they had once tried to have performance plays on television. When they discovered that the inherent properties of virtual reality allowed for much deeper immersion, they knew that they had to adjust the entertainment accordingly. The results were amazing.*

7 General Conclusion

Great books are written at the great junctures of history. When Mankind comes close to finishing one chapter in the book of life and is about to open a new one, we suddenly become aware of the gravity of where we came from, where we are and where we are heading.

In this dissertation, I have tried to bring together two sets of authors who wrote such great books at such great junctures of history.

The first set of authors concerns the classical social contract theorists and it includes well-known names such as Hobbes, Rousseau and Locke. These authors have given Mankind the cornerstones of modern political and legal philosophy and they have helped us understand the relation between Man and State as Mankind was closing our Chapter on the Agricultural Age and started the Chapter on the Industrial Age.

The second set of authors concerns modern theorists of society and technology, and it includes less-known names such as Kurzweil, Kelly and Morris. These authors are giving us the cornerstones of modern and future political and technological philosophy as they are helping us understand the relation between Man and Machine as Mankind is closing our Chapter on the Industrial Age and is starting our Chapter on the Information Age.

Just as was the case with the founders of modern political and legal philosophy in the 17th and 18th century before them, the theorists of today in the 20th and 21st century are greatly aware and involved in each other's works. Although just as with the founders of modern political and legal philosophy, not one of them will individually manage to accurately describe all of this new reality, collectively, they are building an understanding of society without precedent.

This dissertation has tried to bring these two sets of authors together and it has tried to apply the rules from political and legal philosophy from the 17th and 18th centuries to our 21st century to see if the principles which were laid out back then are still relevant for the Information Age. I have demonstrated that the world for which the social contract theorists wrote their works has changed, but that the abstraction behind their works still provides valuable tools for structuring our society in the Information Age. Technology has changed Man and society, but human nature has not changed. Essentially, *Homo sapiens* is still concerned with his life, liberty and property as well as with their collective expressions in the shape of sovereign existence, political independence and territorial integrity. The State remains the best

technology we have invented to guarantee the protection of these interests. *Plus ça change, plus c'est la même chose.*

This dissertation started in Chapter 1 with a retelling of the story of how Hugo Grotius set out his legal theory for what came to be known as the high seas. In this chapter, I discussed the two types of public ownership; ownership by States and ownership as the Common Heritage of Mankind (*res communis*). In this dissertation I have asked whether there are parts of this new space, cyberspace, which, pursuant to social contract theory on State sovereignty must necessarily fall within the ownership of States (*res publica*).

Chapter 3 has set out the framework through which I have approached this question. It has explained why the *raison d'être* of the State is the protection of its citizens from force against their life, liberty and property. In this chapter, I have also argued that the prevalence of the protection of life, liberty and property in philosophy and in law, across time and space, is not a historical coincidence, but rather that it reflects a fundamental logic to structuring a society. As biological beings, we have objective interests dictated, ultimately, by the laws of physics. We require access to energy and materials to rebuild the wear and tear of entropy so that we can survive and reproduce. Any legal system or theory must comply with this natural logic. In addition, in this chapter, I have also argued that in the international legal system, these interests of life, liberty and property, attain a collective form in the shape of sovereign existence, political independence and territorial integrity and that through the social contract between the individual and the State, the State inherits not just a right to monopolize the use of force within its territory, but also the duty to do so, both from internal aggression as well as from external aggression. It must hence protect citizens not just from each other, but also from other States. This too is not a historical coincidence, but reflects a fundamental logic to structuring the society of States. This chapter has concluded that State sovereignty is ultimately derived from the protection of the vital interests of its citizens. Thus, there are two necessary requirements for State sovereignty which need to be fulfilled; 1. A State must exercise effective control over a particular space 2. so that it can provide protection of life, liberty and property as well as their collective representations in the shape of sovereign existence, political independence and territorial integrity.

Chapter 4 has dealt with the question of effective control over the domain of cyberspace and Chapters 5 and 6 have dealt with the question of what it means to protect life, liberty and

property, as well as its collective representations of sovereign existence, political independence and territorial integrity in the Information Age.

Before we can discuss this application of the facts to the framework as set out in Chapter 3, we first have to discuss the factional background. Chapter 2 has defined, delineated and delimitated the domain of cyberspace and it has discussed the importance of the Information Age to Mankind. The chapter has thereto discussed the natural laws of the digital universe. These laws, such as Moore's Law, Kryder's Law and Nielsen's Law shape the constituting dimensions of the digital universe, namely processing power, storage capacity and transmission speed. Moreover, these laws also contribute to the three main trends of the digital universe, namely; acceleration, miniaturization and dematerialization. As the digital universe gets more powerful, smaller and more connected, increasingly powerful, cheap and small sensors, chips, and (wireless) connectivity are leading to the internet of everyone and the internet of everything. A global society is being formed among Mankind and between Man and Machine. In this chapter I have argued that because the defining characteristic of this age is the centrality of information, that we, as Mankind, are about to enter the Information Age. It is an entirely new chapter of civilization, as revolutionary, unique and grand as our previous chapters on our hunter/gatherer, agricultural and industrial ages.

Chapter 4 has dealt with the question of effective control over cyberspace and has thus combined Chapters 2 and 3. The chapter has thereto had to address the attribution problem of cyberspace; the idea that anyone, anywhere can direct a cyber-attack of any scale against anyone, anywhere and that this can be done with complete anonymity. This chapter has used the international legal framework on State responsibility and the Stuxnet case to explore whether responsibility can be attributed to actors for malicious conduct through cyberspace. The chapter has detailed the two requirements which need to be fulfilled for conduct (by commission or by omission) to fall under the responsibility of a State; there has to be *attributability* and there has to be a *breach of an international obligation*. The chapter has subsequently applied these requirements to the domain of cyberspace. In this chapter it was concluded that cyber operations which can meet the use of force threshold to breach the cornerstone of the international legal system; the prohibition on the use of force pursuant to Article 2(4) UN Charter - such as large-scale theft of intellectual property and durable disruption of critical infrastructures, as discussed in Chapters 5 and 6 respectively - can only be conducted under the responsibility of (few) States. Moreover, given the high barriers to entry for attaining the scale and effects to meet the severity threshold for use of force and given the

ways in which exercising coercion is effected, this chapter has argued that this cannot be done with anonymity. As States cannot conduct cyber operations which meet the use of force threshold with anonymity, States against whom such cyber operations have been directed, know who the responsible actor is and can wield the appropriate responses to re-establish effective deterrence and to take an eye for an eye so as to reassert effective control over their cyber territory. The first criteria for State sovereignty over cyberspace has thus been met.

Chapters 5 and 6 have dealt with the second criteria; the protection of the interests of life, liberty and property, as well as their collective representations of sovereign existence, political independence and territorial integrity. Chapter 5 has dealt with the production of intellectual property and Chapter 6 has dealt with providing services through infrastructures.

Chapter 5 has dealt with large-scale theft of intellectual property through cyber operations and it has argued why in the information age this is akin to territorial aggrandizement. Thereto, it has discussed the principles through which ownership is established over physical objects, land and ideas. It started with the state of nature and it explained how among social animals, like *Homo sapiens*, there is ownership over one's labor. It is the mixture of this labor (manual or mental) with *res nullius*, *terra nullius* and, what I have coined *data nullius*, which establishes ownership over physical objects, land and ideas, respectively. This chapter has also argued that, given that we are moving into the Information Age in which our livelihoods increasingly depend on being able to capitalize on the valuable nuggets of information we extract and process from data mines, that the information resources which we have cultivated, need to be regarded analogous to valuable cultivated agricultural fields or natural resource mines. Whereas previously wars would be launched at the aggrandizements of such fields or mines, it has now become more severe for a State to be subject to large-scale theft of intellectual property. Resultantly, wars will now be launched at the aggrandizement of our intellectual property. In sum, this chapter has concluded that the more a State's economy moves into cyberspace and the larger the scale of the theft of intellectual property, the more severe the effects of this theft become and therefore, the more likely it is that a State will consider such theft as aggrandizement of cyber territory.

Chapter 6 has dealt with durable disruption of critical infrastructures through cyber operations and it has argued why this is akin to a blockade. It started with the state of nature and how increasingly moving away from it results in trade and specialization. Subsequently, this trade and specialization leads to the production of technological tools on which we become

dependent. The natural relationship between Man and Machine is a symbiotic one. Technology is an extension of the human body and analogously, infrastructures are the technologies which are the extensions of the State body. Just as with technology and Man, the State becomes dependent upon them and some of them are even critical. In this chapter I have discussed the critical infrastructures of energy, matter and information and I argued that these are respectively analogous to the respiratory-, cardiovascular- and central nervous systems of the State body pursuant to the anatomy analogy. In this chapter, I have also discussed how their increasing connection to cyberspace makes it possible for cyber operations to cause severe durable functional disruptions to the movement of energy, matter and information. Given the dependence of the State on these infrastructures, I have argued that States will respond to such attacks on their bodies as they would to a blockade of energy, matter and information from their territory. In sum, this chapter has concluded that the more a State's critical infrastructures become dependent upon the well-functioning of cyberspace and the more durable the functional disruption which is caused by a cyber operation, the more severe the effects of this disruption become and therefore, the more likely it is that a State will consider such disruption as a blockade of energy, matter or information from its territory.

In sum, I have argued that State sovereignty extends to the domain of cyberspace, because the State remains the necessary guarantor for the protection of its citizens from force against their life, liberty and property as well as their collective representations of sovereign existence, political independence and territorial integrity. People continue to need the State to provide the protection from cyber operations aimed against them by foreign States and which result in large-scale theft of intellectual property or durable disruption of critical infrastructures. States are the natural way to protect the vital interests of people, and I have demonstrated that this remains the case in the Information Age.

The nation State remains the best vehicle for elevating the human condition.

I will leave this dissertation with another transcript from the Matrix trilogy:

"Neo*:* *I thought it wasn't real*

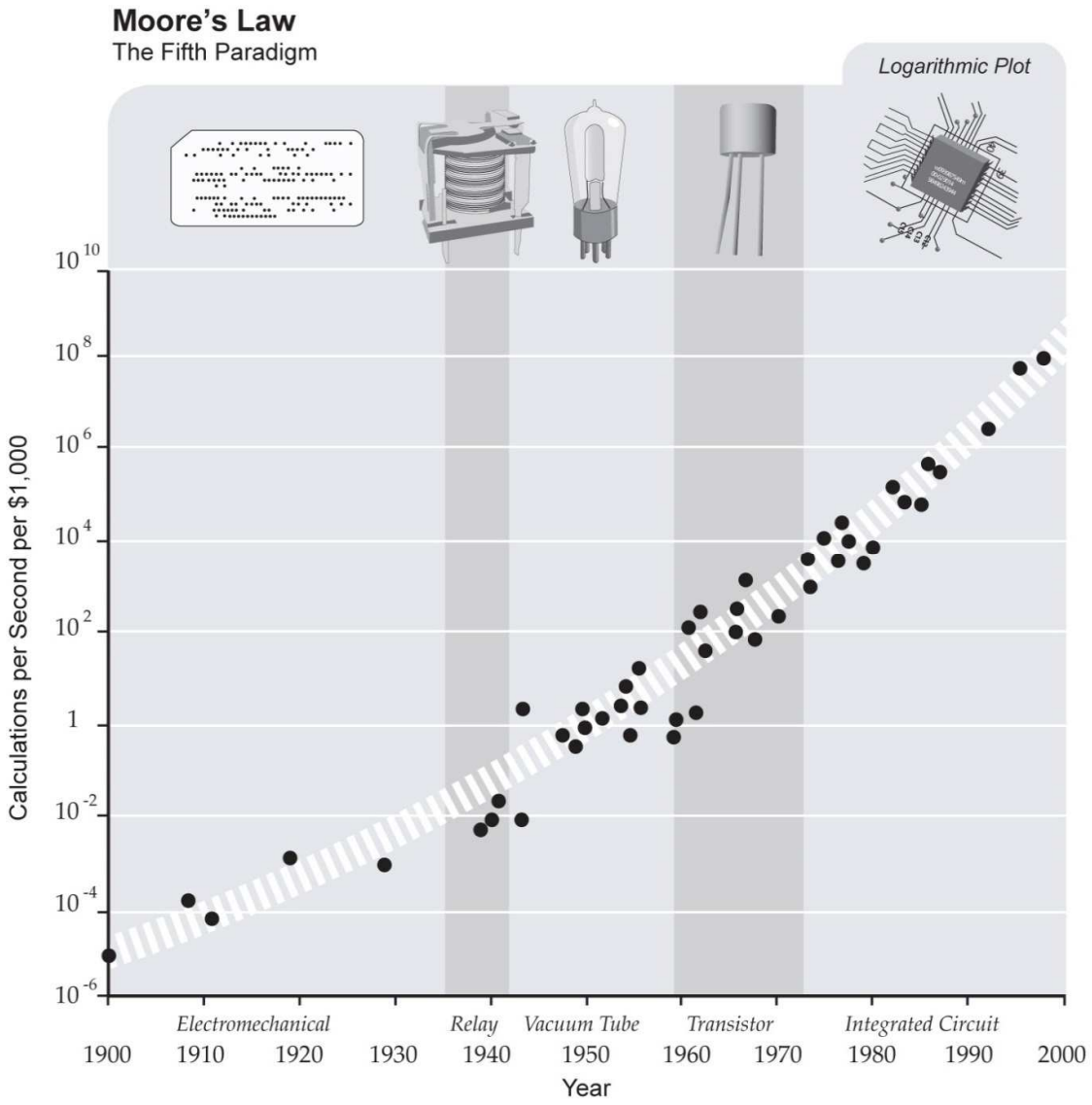
Morpheus*:* *Your mind makes it real*

Neo*:* *If you're killed in the matrix, you die here?*

Morpheus*:* *The body cannot live without the mind."*[570]

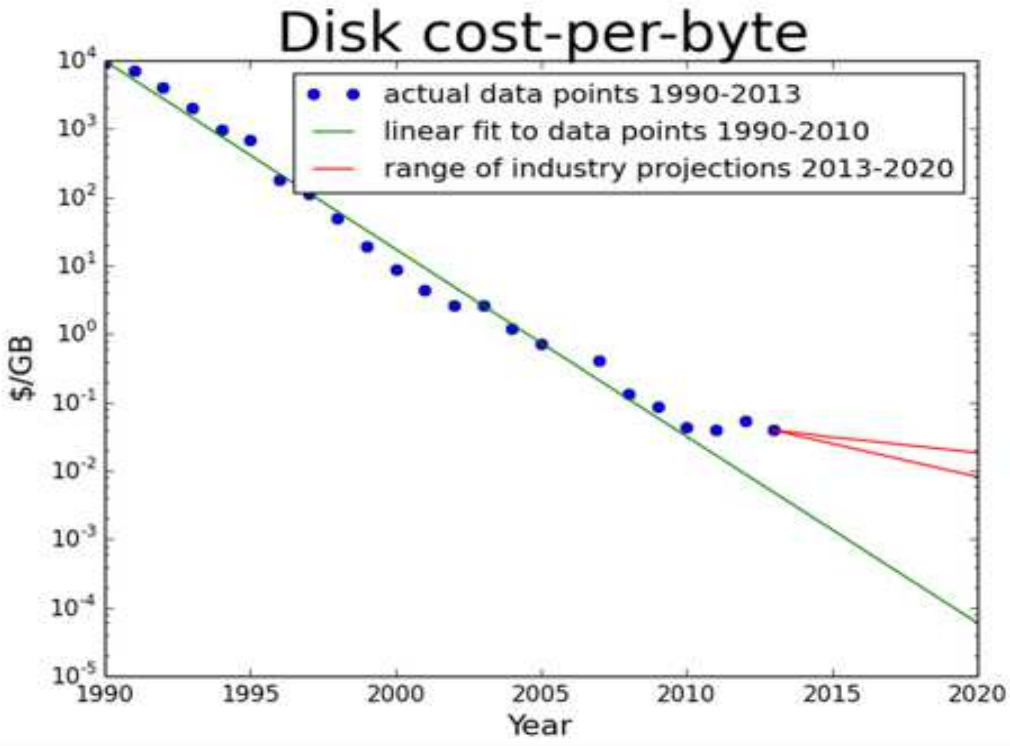
[570] The Matrix (1999), part 4.

Appendix 1. The Natural Laws of the Digital Universe: Processing power[571]



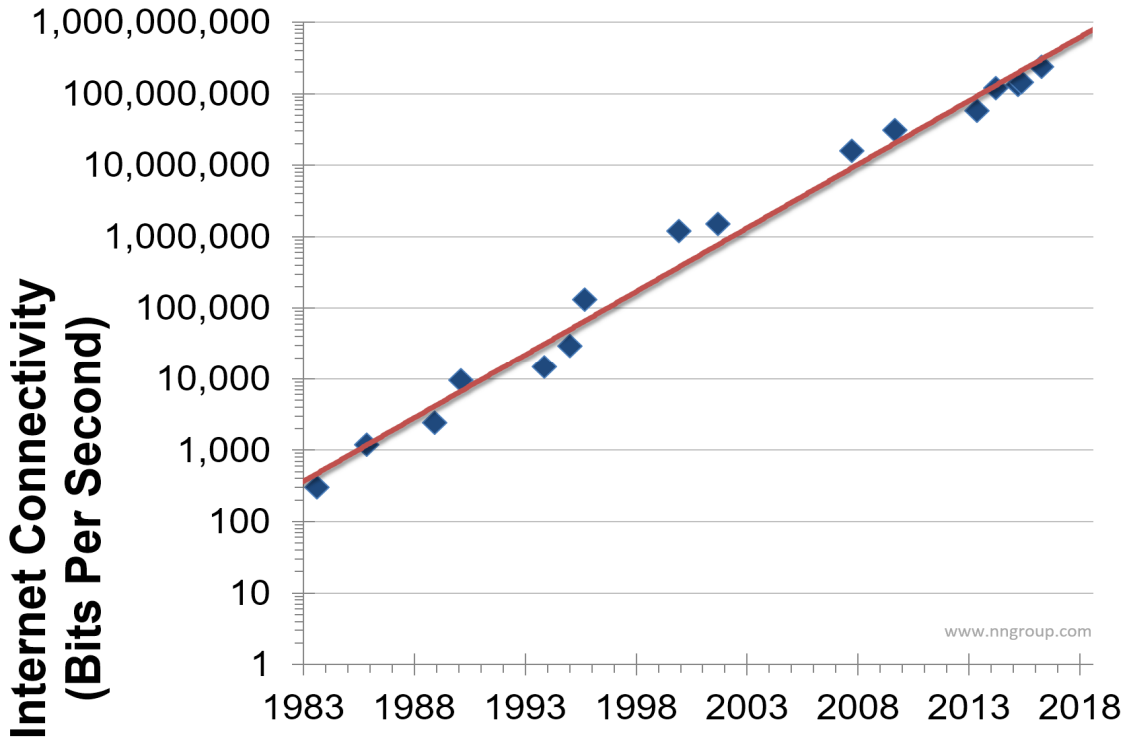
[571] Moore's Law, In: *Wikipedia*, available at: https://en.wikipedia.org/wiki/Moore%27s_law (accessed on 31st July, 2017).

Appendix 2. The Natural Laws of the Digital Universe: Storage Capacity[572]



[572] *See* C. Walter, Kryder's Law, Scientific American, 1st August, 2005, available at: https://www.scientificamerican.com/article/kryders-law/ (accessed on 31st July, 2017).

Appendix 3. The Natural Laws of the Digital Universe: Transmission Speed[573]



[573] J. Nielsen, Nielsen's Law of Internet Bandwidth, 5th April 1998, available at: https://www.nngroup.com/articles/law-of-bandwidth/ (accessed on 31st July, 2017).

Dutch Summary

Digitale Kracht: *Leven, Vrijheid en Levensonderhoud in het Informatie Tijdperk*

Deze dissertatie heeft getracht om twee ogenschijnlijk onverenigbare concepten met elkaar te verenigen, te weten; de politieke filosofie die ten grondslag ligt aan de fysiek begrensde entiteit van de Staat en de inherente grenzenloosheid van de digitale wereld.

De wereld van Staten is een wereld die tot stand kwam in de 16de eeuw in Europa en die sindsdien de dominante vorm van sociale organisatie is geweest. In deze wereld leven volkeren in een afgebakend fysiek gebied waar zij anderen lang genoeg succesvol met geweld van hebben weten te weren. Bekeken vanuit de ruimte zien we dat deze afbakeningen veelal langs natuurlijke barrières zijn gevormd; bergen, dalen, woestijnen, bossen, zeeën en rivieren dicteren de grenzen tussen de ene staat en de andere. Het is een wereld veelal van dwang.

De digitale wereld daarentegen is een wereld die tot stand kwam in de 20ste eeuw en die steeds dominanter wordt als vorm van sociale organisatie. In deze wereld leven alle volkeren min of meer in éénzelfde ruimte. Aangezien deze wereld niet fysiek is, zijn er ook geen grenzen

die fysiek bevochten kunnen worden. De digitale wereld is een min of meer globale wereld die veelal georganiseerd is op basis van vrijwilligheid.

De centrale onderzoeksvraag waarin deze twee werelden zijn samen gebracht, luidt:

Kan de sociaal contract theorie over staatssoevereiniteit worden toegepast op het cybergebied?

Deze vraag is in deze dissertatie behandeld in 4 delen over 7 hoofdstukken. Deel 1 beslaat de hoofdstukken 1 en 2 en heeft tot doel de lezer te introduceren in het probleem en in de feitelijke situatie. In deel 2 (bestaande uit hoofdstuk 3) wordt het politiek filosofische raamwerk uiteengezet waaraan de feitelijke situatie later getoetst wordt. In Deel 3 (bestaande uit hoofdstukken 4 tot en met 6) wordt dit politiek filosofische raamwerk vervolgens getoetst aan de feitelijke situatie zoals beschreven in hoofdstuk 2. In deel 4 (bestaande uit hoofdstuk 7) wordt afgesloten met enkele algemene conclusies en afsluitende observaties.

Hoofdstuk 2 bevat, zoals gezegd, een feitelijk overzicht van de definitie, afbakening en begrenzing van het cybergebied. Daartoe bevat dit hoofdstuk eerst een historisch overzicht van de opkomst van het digitale universum en van het cybergebied. Vervolgens zijn de drijvende krachten of 'natuurwetten' van het digitale universum uitgelegd. Daarna zijn deze natuurwetten van het digitale universum vooruit geprojecteerd, de toekomst in. In dit hoofdstuk wordt beargumenteerd dat ten gevolge van de natuurwetten van het universum, dat het 'Informatie Tijdperk' zal aanbreken voor de mensheid. Tevens wordt hierin aangeven welke terminologie in relatie tot het cyber domein wordt gehanteerd en wat de relevantie hiervan is voor het verhaal van de mensheid.

Hoofdstuk 3 verkent de voorwaarden waaronder Staten gebied kunnen incorporeren als onderdeel van hun soevereine domein. Vertrekkend vanuit de natuurtoestand wordt uitgelegd hoe deze natuurlijk- en logischerwijs leidt tot een oorlog van allen tegen allen. Vervolgens wordt beschreven hoe die natuurtoestand natuurlijk- en logischerwijs zal leiden tot de wetten van mensen op basis van de overeenkomst om geen geweld te gebruiken tegen andere deelnemers van de overeenkomst. Daarna wordt uitgelegd hoe vanuit deze overeenkomst natuurlijk- en logischerwijs een noodzaak ontstaat tot een neutrale arbiter die deze overeenkomst kan afdwingen en waarom dit leidt tot de oprichting van een centrale Staat die

geweld monopoliseert. Er wordt beargumenteerd dat staatssoevereiniteit een geweldsmonopolie vereist over soevereine ruimtes – zoals grond-, water-, lucht- en cybergebied – zodat de Staat de levens, vrijheid en eigendommen van zijn burgers kan beschermen, zowel in hun individuele vorm, als ook in hun collectieve vorm als soevereine existentie, politieke onafhankelijkheid en territoriale integriteit.

Hoofdstuk 4 richtte zich op de eerste voorwaarde die geformuleerd is in hoofdstuk 3, te weten het vermogen om geweld effectief te monopoliseren. Wanneer Staten zouden falen in het monopoliseren van geweld in een bepaalde ruimte – zoals het cybergebied – dat gericht is tegen de levens, de vrijheid en de eigendommen van burgers of dat gericht is tegen het soevereine bestaan, de politieke onafhankelijkheid en de territoriale integriteit van de Staat, dan zou de discussie over Staatssoevereiniteit in dit gebied verder zinloos zijn. Een Staat geweld effectief monopoliseren in een bepaald gebied om in dat gebied de soeverein te zijn. Dit hoofdstuk heeft daarom verkend of het mogelijk is voor Staten om geweld te monopoliseren in het cybergebied, zoals gedefinieerd, afgebakend en begrens in hoofdstuk 2. In dit hoofdstuk wordt beargumenteerd dat het zogenaamde 'attributie probleem' – welke het gevolg is van de inherente anonimiteit van het cybergebied – opgelost kan worden wanneer het gaat om cyber operaties die de 'ernst-drempel' van geweldsgebruik halen en wordt uitgelegd waarom deze dissertatie zich exclusief richt op de handelingen van Statelijke actoren. Aan het einde van het hoofdstuk wordt geconcludeerd dat Staten daadwerkelijk in staat zijn om het geweldsmonopolie te vestigen in die delen van het cybergebied die vallen binnen hun soevereine domein aangezien cyber operaties die de ernst drempel voor geweldsgebruik kunnen bereiken, in de regel genomen niet anoniem verricht kunnen worden.

De hoofdstukken 5 en 6 richtten zich op de tweede voorwaarde van Staatssoevereiniteit zoals geformuleerd in hoofdstuk 3, te weten de bescherming van leven, vrijheid en eigendom en hun collectieve vormen van soevereine existentie, politieke onafhankelijkheid en territoriale integriteit.

Hoofdstuk 5 wordt de juridische en morele grondslag van eigendom aan een nader onderzoek onderworpen. Uiteen wordt gezet hoe eigendom verkregen kan worden over voorwerpen, land en ideeën, welke respectievelijk gevormd zijn uit *res nullius*, *terra nullius* en *data nullius*. Vervolgens wordt beargumenteerd dat, aangezien in het Informatie Tijdperk waarde voornamelijk wordt gecreëerd in het cybergebied, dat Staten het deel van het cybergebied waar hun burgers waarde creëren, dienen te beschouwen als onderdeel van hun

soevereine cybergebied. Dientengevolge wordt gesteld dat grootschalige diefstal van intellectuele eigendommen middels cyber operaties als even ernstig beschouwd dient te worden als territoriale expansie in schending van de territoriale integriteit middels traditionele, fysieke operaties, zoals (dreigen tot) grootschalig gebruik van geweld onder vlag van een andere staat (zoals aanvallen van de landmacht, marine of luchtmacht).

Hoofdstuk 6 bespreekt de relatie tussen Mens en Machine. Hierin wordt beargumenteerd dat technologie gezien dient te worden als een verlengstuk van het menselijke lichaam en dat middels een anatomie analogie kritieke infrastructuren gezien dienen te worden als een verlengstuk van het Staatslichaam met hierbij de infrastructuren voor energie, materialen en informatie functionerende als, respectievelijk, het ademhalingssysteem, het cardiovasculaire systeem en het zenuwstelsel van het staatslichaam. Gelet op de symbiotische relatie tussen Mens en Machine en tussen Staat en kritieke infrastructuren, wordt beargumenteerd in dit hoofdstuk dat duurzame verstoring van kritieke infrastructuren middels cyber operaties als even ernstig beschouwd dient te worden als een blokkade van de Staat middels traditionele, fysieke operaties, zoals (dreigen tot) grootschalig gebruik van geweld onder vlag van een andere staat (zoals aanvallen van de landmacht, marine of luchtmacht).

Hoofdstuk 7 tenslotte vormt het sluitstuk van de dissertatie. Hierin worden de voorafgaande hoofdstukken samengevat en wordt afgesloten met enkele afsluitende observaties en aanbevelingen.

Samengevat heb ik in deze dissertatie beargumenteerd dat bezien vanuit de politieke filosofie van het sociaal contract denken over Staatssoevereiniteit, dat het soevereine domein reikt over het cybergebied, aangezien de staat de beste beschermer blijft van zijn burgers voor geweld tegen hun leven, vrijheid en eigendom. Mensen blijven de Staat nodig hebben in de bescherming tegen cyber operaties die tegen hen gericht zijn onder vlag van een andere Staat wanneer deze operaties resulteren in grootschalige diefstal van intellectuele eigendomen of in duurzame verstoring van kritieke infrastructuren. Staten zijn de natuurlijke manier waarop mensen hun essentiële belangen beschermen en ik heb aangetoond dat dit onveranderd is in het Informatie Tijdperk.

Bibliography

Books

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

Brynjolfsson, E., & McAfee, A. (2011). Race against the machine: how the digital revolution is accelerating innovation, driving productivity, and irreversibly transforming employment and the economy. Lexington, Massachusetts, Digital Frontier Press.

Bynkershoek, C. V., Magoffin, R. V. D., & Scott, J. B. (1923). *De dominio maris dissertatio: in one volume*. Opera Minora / Cornelius Van Bijnkershoek, 2nd Ed., 1744, S. 352 - 429. Buffalo, NY, HeinOnline. http://heinonline.org.

Dyson, G. (2012). Turing's cathedral: the origins of the digital universe. New York, Pantheon Books.

Dawkins, R. (2016). *The selfish gene.* Oxford, Oxford University Press.

Diamond, J. (1997). *Guns, Germs, and Steel*. New York, W.W. Norton & Co.

Diamandis, P. H., & Kotler, S. (2012). *Abundance: the future is better than you think.* New York, NY [u.a.], Free Press.

Dinstein, Y. (2011). *War, Aggression and Self-Defence*. New York. Cambridge University Press.

Ehrlich, P. R. (1968). *The population bomb.* New York. Rivercity Press.

Eyffinger, A (2008). *Self-Defence as a Fundamental Principle*. The Hague, Hague Academic Press.

Fourastie, J. (1949). *Grand espoir du XX Siecle.* Paris, Presses Universitaires de France

Gladwell, M. (2000). *The tipping point. How little things can make a big difference*. Boston, Little, Brown.

Grotius, H., 1916. *The Freedom of the Seas, or the Right Which Belongs to the Dutch to Take Part in the East Indian Trade.* New York: Oxford University Press.

Heck, S., Rogers, M., & Carroll, P. (2014). *Resource revolution: how to capture the biggest business opportunity in a century.* Boston, Houghton Mifflin Harcourt.

Hobbes, T. (1651). *Leviathan: or The matter, form, & power of a common-wealth ecclesiastical and civil*. Project Gutenberg EBook of Leviathan, by Thomas Hobbes

Kelly, K. (2010). *What technology wants*. New York, Viking.

Kelly K. (2016). *The inevitable: understanding the 12 technological forces that will shape our future.* New York, Viking.

Kipling, R. (1894). *The jungle book*. Garden City, N.Y., Doubleday.

Kurzweil, R. (2005). T*he singularity is near: when humans transcend biology.* New York, Penguin Books.

Locke, J. (2017). Second Treatise of Government. [S.l.], Project Gutenberg EBook of Second Treatise of Government, by John Locke.

Lovins, A. B., Odum, M., & Rowe, J. W. (2013). *Reinventing fire: bold business solutions for the new energy era*. White River Junction, VT, Chelsea Green Publishing.

McLuhan, M., Gordon, W. T., Lamberti, E., & Scheffel-Dunand, D. (2017). *The Gutenberg galaxy: the making of typographic man.* Toronto, University of Toronto Press.

Morris, I. (2010). *Why the West rules ... for now: the patterns of history, and what they reveal about the future*. New York, N.Y., Farrar, Straus & Giroux.

Morris, I. (2013). *The Measure of Civilization: How Social Development Decides the Fate of Nations.* Princeton, Princeton University Press.

Naam, R. (2013). *The infinite resource: the power of ideas on a finite planet.* Hanover, NH [u.a.], Univ. of New England Press.

Pinker, S. (2012). *The better angels of our nature: a history of violence and humanity.* London, Penguin Books.

Reed, L. W., & Friedman, M. (2008). *I, pencil: my family tree as told to Leonard E. Read.* Irvington-on-Hudson, Foundation for Economic Education.

Rid, T. (2013). *Cyber War Will Not Take Place*. C. Hurst & Co.

Ridley, M. (2011). *The rational optimist: how prosperity evolves.* New York, Harper Perennial.

Rousseau, J.J., (1751). *Discourse on Inequality.* Project Gutenberg EBook of Discourse on Inequality, by Jean Jacques Rousseau.

Rousseau, J.J. (2016). *The social contract.* Project Gutenberg EBook of The Social Contract, by Jean Jacques Rousseau.

Ruys, T. (2010), *'Armed Attack' and Article 51 of the UN Charter – Evolutions in Customary Law and Practice*. New York, Cambridge University Press.

Sanger, D. (2012). *Confront and Conceal: Obama's Surprising Use of American Power*. New York. Random House.

Schmidt, E., & Cohen, J. (2013). *The new digital age: reshaping the future of people, nations and business.* New York, Alfred A. Knopf.

Schwab, K. (2017). *The fourth industrial revolution*. New York, N.Y., Crown Business

Schmitt, M. N. (2015). *Tallinn manual on the international law applicable to cyber warfare*: prepared by the International group of experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence. Cambridge, Cambridge University Press.

Schmitt, M.N. (2017), *Tallinn manual 2.0 on the international Law applicable to cyber operations*: prepared by the International group of experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence. Cambridge, Cambridge University Press.

Service, E. R. (1962). *Primitive social organization: an evolutionary perspective*. New York, Random House.

Siegel, S. M. (2015). Let there be water: Israel's solution for a water-starved world. New York, St. Martin's Press.

Simma, B. (2002). *The Charter of the United Nations: A Commentary* (2002), Oxford University Press,

Simon, J. L. (1981). *The ultimate resource. Princeton*, New Jersey, Princeton Univ. Press.

Smith, A. (1776). *An inquiry into the nature and causes of the wealth of nations. Vol. I* London, Printed for W. Strachan and T. Cadell.

Teson, F. R. (1998). *A philosophy of international law: a human rights approach*. Boulder, Colo, Westview.

Waal, F. B. M. D. (2007). *Chimpanzee politics power and sex among apes*. Baltimore, Johns Hopkins Univ. Press.

Walzer, M. (2006). *Just and unjust wars: a moral argument with historical illustrations.* New York, N.Y., Basic.

Yahweh, *The Holy Bible*. King James Version.

Zetter, K. (2015). *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. New York. Penguin Random House.

Articles

Boer, L. (2015). 'Echoes of Times Past'*: On the Paradoxical Nature of Article 2(4), *Journal of Conflict & Security Law*, Vol. 20 No. 1, 5-26.

Foltz, A. (2012). Stuxnet, Schmitt Analysis, and the Cyber "Use-of-Force" Debate, *JFQ*, 67, 2012 – 4.

Maslow, A. H. (1943). A theory of human motivation. *Psychological Review*. 50, 370-396.

Schmitt, M. N. (1999). Computer network attack and the use of force in international law: thoughts on a normative framework. *Columbia Journal of Transnational Law*. 37, 885-937.

Rid, T. & Buchanan, B. (2015). Attributing Cyber Attacks, *Journal of Strategic Studies*. 38:1-2, 4-37.

Stone, J. (2013). Cyber War Will Take Place, *Journal of Strategic Studies*. 36:1, 101-108.

Turing, A. M. (1937). On computable numbers: with an application to the Entscheidungsproblem. *Proceedings of the London Mathematical Society*. 42, 3-4.

Online sources

Ashton, K. (2009). RFID Journal. [Online]
Available at: http://www.rfidjournal.com/articles/view?4986
[Accessed 31 July 2017].

Barlow, J. P. (1996). A declaration of the independence of cyberspace. San Francisco, CA, Electronic Frontier Foundation. [Online]
Available at: http://homes.eff.org/~barlow/Declaration-Final.html.
[Accessed 31 July 2017]

Department of Defense Office of General Counsel. (1999). *An Assessment of International Legal Issues in Information Operations.* [Online]

Available at: http://www.fas.org/irp/eprint/io-legal.pdf
[Accessed 31 July 2017]

Dubner, S. & Levitt,S. (2005). *Monkey Business.* [Online]
Available at: http://www.nytimes.com/2005/06/05/magazine/monkey-business.html
[Accessed 31 July 2017]

Krauss, L M, & Starkman, G D. (2004). Universal Limits on Computation.
http://documents.cern.ch/cgi-bin/setlink?base=preprint&categ=astro-ph&id=0404510.

[Accessed 31 July 2017]

Langner, R., 2010. *Ralph's Step-by-Step Guide to Get a Crack at Stuxnet Traffic and Behavior*. [Online] Available at: https://www.langner.com/2010/09/ralphs-step-by-step-guide-to-get-a-crack-at-stuxnet-traffic-and-behavior/
[Accessed 31 July 2017]

Morgan, S., 2015. *Cybersecurity Market Reaches $75 Billion In 2015; Expected To Reach $170 Billion By 2020* [Online] 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]

Nielsen, J., 1998. *Nielsen's Law of Internet Bandwith.* [Online]
Available at: https://www.nngroup.com/articles/law-of-bandwidth/
[Accessed 31 July 2017].

Open Innovation: Goldcorp Challenge, Idea Connection (2009). [Online]
Available at: https://www.ideaconnection.com/open-innovation-success/Open-Innovation-Goldcorp-Challenge-00031.html
[Accessed 31 July 2017]

Sanger, D., 2012. *Obama Order Sped Up Wave of Cyberattacks Against Iran*, New York Times. [Online]
Available at: http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html
[Accessed 31 July 2017].

Shirky, C., 2012. *How the Internet will (one day) transform government.* [Online]
Available at:
http://www.ted.com/talks/clay_shirky_how_the_internet_will_one_day_transform_government
[Accessed 31 July 2017].

Walter, C., 2005. *Scientific American.* [Online]
Available at: https://www.scientificamerican.com/article/kryders-law/
[Accessed 31 July 2017].

International documents

1926 Convention to Suppress the Slave Trade and Slavery.

1945 Charter of the United Nations.

1945 Statute of the International Court of Justice.

1948 United Nations Declaration of Human Rights.

1950 European Convention on Human Rights.

1962 Convention on the High Seas.

1964 Convention on the Continental Shelf.

1964 Convention on the Territorial Sea and Contiguous Zone.

1966 Convention on Fishing and Conservation of the Living Resources of the High Seas.

1967 Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies.

1969 Vienna Convention on the Law of Treaties.

1974 Definition of Aggression.

1976 International Covenant on Civil and Political Rights.

1982 United Nations Convention on the Law of the Sea.

1987 Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment.

Cases

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), 12 May 1981.

Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Merits, Judgment of 27 June 1986, 1986 ICJ Rep. 14.

Prosecutor v. Dusko Tadic (Appeal Judgement), IT-94-1-A, International Criminal Tribunal for the former Yugoslavia (ICTY), 15 July 1999.

Oil Platforms (Islamic Republic of Iran v. United States of America), Judgment of 6 November 2003, 2003 ICJ Rep. 161.

Multimedia

Matrix reloaded. 2014. [Film] Directed by Wachowski L.

The Matrix. 1999. [Film] Directed by Wachowski, L., & Wachowski, L.

Tron: Legacy. 2010. [Film] Directed by Joseph Kosinski.

Other

General Electric, n.d. *Industrial Internet.* [Online]
Available at: https://www.ge.com/digital/industrial-internet
[Accessed 31 July 2017].

Shakespeare, W. *The Merchant of Venice.* Act 4, Scene 1, Page 15-16, lines 338-369. [Online]
Available at: http://nfs.sparknotes.com/merchant/page_190.html
[Accessed 31 July 2017]

Wikipedia, n.d. *Moore's Law*. [Online]
Available at: https://en.wikipedia.org/wiki/Moore%27s_law
[Accessed 31 July 2017].

Curriculum vitae

Roy van Keulen was born on July 18th, 1986 in Beverwijk. Mr. Van Keulen attended Hageveld College in Heemstede, where he followed an Economics & Society profile. After high school, Mr. Van Keulen studied at Leiden University, where he obtained a bachelor's degree in Dutch Law, a master's degree in Public International Law and a master's degree in Philosophy of Law. For his combined master thesis, Roy van Keulen received the Leiden Law School thesis award.