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

Keulen, R.J.F. van

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.