Cyber Attacks and International Law on the Use of Force: an Informational Approach

Samuli Haataja

Bachelor of Laws (First Class Honours) (Griffith University)
Bachelor of International Relations (Griffith University)

Griffith Law School
Arts, Education and Law Group
Griffith University

Submitted in fulfilment of the requirements of the degree of
Doctor of Philosophy

August 2016
Abstract

This thesis examines the intersection of law and technology in the context of cyber attacks and international law on the use of force. It is argued that the law embodies an ontologically constrained view of violence which limits its capacity to regulate cyber attacks. As a means of overcoming these constraints, this thesis draws on Luciano Floridi’s information ethics to develop an informational approach. This involves depicting the state as an information entity and reconceptualising violence through the concept of entropy. Therefore, by updating the law with an informational ontology, it is argued that the law is better equipped to recognising the novel forms of informational violence that are capable of harming states.

As such, this thesis explores the conceptual challenges brought about by technological change for international law on the use of force. As a central provision of international law, Article 2(4) of the United Nations Charter prohibits states from using force in their international relations. The law arose within a particular technological context and was originally intended to limit the outbreak of violent warfare between states. It is argued however, that the law is premised on an anthropocentric and materialist view of what constitutes violence and the state as an entity. It subscribes to a worldview in which the state is a territorial entity and violence that is deemed to threaten the state requires some form of destruction or damage to physical objects or injury or death to human beings.

Where cyber attacks have material effects, such as damage to computer hardware or physical injury to human beings, they are easy to analogous to forms of violence that Article 2(4) is concerned with. However, where cyber attacks have non-material effects, such as damage to information or disruption of information processes, they are generally considered as potential breaches of the non-intervention principle alone and effectively depicted as forms of non-violence. It is argued that the law’s worldview, its ontology, limits its capacity to recognise cyber attacks with non-material effects as a form of violence. As such, the law is unable to adequately account for the informational harm that non-material cyber attacks can cause to states as information societies.

In order to overcome the law’s ontological constraints, this thesis draws on Floridi’s information ethics. Information ethics adopts an informational ontology and provides a form of environmental ethics that is concerned with the wellbeing of the infosphere – the entire
informational environment constituted by all information entities, whether real or virtual, natural or artificial, human or non-human. Using this framework and through two case studies, this thesis develops an informational approach to the law on the use of force and cyber attacks. This involves reconceptualising the state as an information entity and the notion of violence through the concept of entropy. It is argued that by doing so, the law can be updated to recognise a broader spectrum of violence. As such, even non-material forms of informational violence that undermine the informational integrity of the state or disrupt its functioning as an entity, can be recognised as capable of harming the state.
Statement of Originality

This work has not previously been submitted for a degree or diploma in any university. To the best of my knowledge and belief, the thesis contains no material previously published or written by another person except where due reference is made in the thesis itself.

____________________________
Samuli Haataja
Contents

Abstract ........................................................................................................................................... ii
Statement of Originality .................................................................................................................. v
Contents ........................................................................................................................................... vii
List of Tables ................................................................................................................................... xi
List of Abbreviations ..................................................................................................................... xii
Acknowledgements ...................................................................................................................... xiv
Chapter 1: Introduction .................................................................................................................. 1
An Overview of Information Ethics ............................................................................................... 8
Research Question and Methodology ........................................................................................... 10
Overview of Thesis ......................................................................................................................... 12
Chapter 2: Information Ethics ...................................................................................................... 17
Introduction ..................................................................................................................................... 17
Section 1: The Philosophies of Technology and Information ..................................................... 17
  1.1 Philosophy of Technology ....................................................................................................... 17
  1.2 Luciano Floridi’s Philosophy of Information ......................................................................... 20
    1.2.1 The fourth revolution and the ‘reontologisation’ of the infosphere .............................. 22
  1.3 The Impact of ICTs and the turn to Information Ethics ........................................................ 24
Section 2: Information Ethics ...................................................................................................... 25
  2.1 Information Entities and the Infosphere ................................................................................ 26
  2.2 The Ontological Equality Principle ...................................................................................... 29
  2.3 Goodness/Being and Evil/Entropy ....................................................................................... 30
  2.4 Criticisms ............................................................................................................................... 33
    2.4.1 The ontological equality principle and value conflicts ............................................... 33
    2.4.2 Entropy as evil ............................................................................................................... 35
    2.4.3 Floridi’s responses ........................................................................................................... 36
Conclusion ....................................................................................................................................... 38
Chapter 3: Technology, Violence, and Law .............................................................................. 40
Introduction ..................................................................................................................................... 40
Section 1: International Law and Information ............................................................................ 40
Section 2: International Law and the Containment of Violence ............................................... 48
  2.1 Violence, the State, and Law ................................................................................................. 48
2.2 Technology .............................................................................................................56

Section 3: Cyber Attacks and the Containment of Violence ........................................58

3.1 The Novel Nature of Cyber Warfare ...................................................................59

3.1.1 Entities .............................................................................................................60

3.1.2 Environment ....................................................................................................61

3.1.3 Harm and violence ........................................................................................62

Section 4: An Informational Approach ......................................................................64

4.1 State .....................................................................................................................65

4.2 Violence ...............................................................................................................69

4.3 Law .......................................................................................................................73

Conclusion ................................................................................................................74

Chapter 4: Cyber Attacks and International Law ......................................................76

Introduction ..............................................................................................................76

Part 1: The Use of Force and Non-Intervention .......................................................76

Section 1: The Use of Force .....................................................................................76

Section 2: Non-Intervention .....................................................................................88

Part 2: Cyber Attacks, the Use of Force, and Non-Intervention .............................93

Section 1: Cyber Attacks and the Use of Force .......................................................93

Section 2: Cyber Attacks and Non-Intervention ....................................................104

Conclusion ..............................................................................................................107

Chapter 5: Estonia ..................................................................................................110

Introduction ............................................................................................................110

Section 1: Events .....................................................................................................111

1.1 Background and Overview ..............................................................................111

1.2 Events .................................................................................................................114

1.3 Attack Methods ................................................................................................117

1.4 Effects ................................................................................................................121

1.5 Estonian Defences ..............................................................................................122

1.6 Estonian Responses and Russian Involvement ...............................................123

Section 2: The Ontological Constraints of the Law .............................................127

2.1 Estonia and the Use of Force Threshold ............................................................128

Section 3: An Informational Approach ..................................................................133

3.1 The Estonian Entity ..........................................................................................134
<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.2</td>
<td>Entropy</td>
<td>136</td>
</tr>
<tr>
<td>3.3</td>
<td>Informational Violence and International Law</td>
<td>140</td>
</tr>
<tr>
<td>Conclusion</td>
<td></td>
<td>142</td>
</tr>
<tr>
<td><strong>Chapter 6: Stuxnet</strong></td>
<td></td>
<td>145</td>
</tr>
<tr>
<td>Introduction</td>
<td></td>
<td>145</td>
</tr>
<tr>
<td>Section 1: Events</td>
<td></td>
<td>146</td>
</tr>
<tr>
<td>1.1 Media Reports</td>
<td></td>
<td>146</td>
</tr>
<tr>
<td>1.2 Technical Design</td>
<td></td>
<td>149</td>
</tr>
<tr>
<td>1.3 The Non-Proliferation Treaty and the Uranium Enrichment Process</td>
<td>151</td>
<td></td>
</tr>
<tr>
<td>1.4 Propagation Methods</td>
<td></td>
<td>153</td>
</tr>
<tr>
<td>1.5 The Payload</td>
<td></td>
<td>158</td>
</tr>
<tr>
<td>1.6 Iran’s Responses and the Effects of Stuxnet</td>
<td>160</td>
<td></td>
</tr>
<tr>
<td>1.6.1 Iran’s responses</td>
<td></td>
<td>160</td>
</tr>
<tr>
<td>1.6.2 The IAEA’s reports</td>
<td></td>
<td>161</td>
</tr>
<tr>
<td>1.6.3 Effects</td>
<td></td>
<td>163</td>
</tr>
<tr>
<td>Section 2: The Ontological Constraints of the Law</td>
<td>163</td>
<td></td>
</tr>
<tr>
<td>2.1 Stuxnet and the Use of Force Threshold</td>
<td>164</td>
<td></td>
</tr>
<tr>
<td>Section 3: An Informational Approach</td>
<td>168</td>
<td></td>
</tr>
<tr>
<td>3.1 The Iranian Entity and the Natanz System</td>
<td>169</td>
<td></td>
</tr>
<tr>
<td>3.2 Stuxnet and Entropy</td>
<td></td>
<td>173</td>
</tr>
<tr>
<td>3.2.1 Propagation methods</td>
<td></td>
<td>173</td>
</tr>
<tr>
<td>3.2.2 Man-in-the-middle</td>
<td></td>
<td>176</td>
</tr>
<tr>
<td>3.2.3 Payload</td>
<td></td>
<td>177</td>
</tr>
<tr>
<td>3.2.4 The Iranian entity’s responses</td>
<td></td>
<td>178</td>
</tr>
<tr>
<td>3.3 Physical and Informational Violence, and International Law</td>
<td>180</td>
<td></td>
</tr>
<tr>
<td><strong>Chapter 7: Conclusion</strong></td>
<td></td>
<td>184</td>
</tr>
<tr>
<td>Thesis Overview</td>
<td></td>
<td>185</td>
</tr>
<tr>
<td>Information Ethics</td>
<td></td>
<td>188</td>
</tr>
<tr>
<td>International Law</td>
<td></td>
<td>190</td>
</tr>
<tr>
<td>Law and Informational Violence</td>
<td></td>
<td>191</td>
</tr>
<tr>
<td>An Informational Approach</td>
<td></td>
<td>194</td>
</tr>
<tr>
<td><strong>Bibliography</strong></td>
<td></td>
<td>198</td>
</tr>
<tr>
<td>Secondary Sources</td>
<td></td>
<td>198</td>
</tr>
<tr>
<td>Section</td>
<td>Page</td>
<td></td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>------</td>
<td></td>
</tr>
<tr>
<td>Primary Sources</td>
<td>225</td>
<td></td>
</tr>
<tr>
<td>Cases, Treaties and Legislation</td>
<td>225</td>
<td></td>
</tr>
<tr>
<td>United Nations Documents</td>
<td>227</td>
<td></td>
</tr>
<tr>
<td>Newspapers and Magazines</td>
<td>229</td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td>235</td>
<td></td>
</tr>
</tbody>
</table>
List of Tables

Table 1: Timeline of attacks, methods and sophistication................................................. 116
# List of Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASIO</td>
<td>Australian Security and Intelligence Organisation</td>
</tr>
<tr>
<td>BOM</td>
<td>Bureau of Meteorology</td>
</tr>
<tr>
<td>CERT</td>
<td>Computer Emergency Response Team</td>
</tr>
<tr>
<td>DDoS</td>
<td>Distributed Denial of Service</td>
</tr>
<tr>
<td>DNS</td>
<td>Domain Name System</td>
</tr>
<tr>
<td>DoS</td>
<td>Denial of Service</td>
</tr>
<tr>
<td>EU</td>
<td>European Union</td>
</tr>
<tr>
<td>GGE</td>
<td>Group of Governmental Experts</td>
</tr>
<tr>
<td>IAEA</td>
<td>International Atomic Energy Agency</td>
</tr>
<tr>
<td>ICANN</td>
<td>Internet Corporation for Assigned Names and Numbers</td>
</tr>
<tr>
<td>ICJ</td>
<td>International Court of Justice</td>
</tr>
<tr>
<td>ICMP</td>
<td>Internet Control Message Protocol</td>
</tr>
<tr>
<td>ICT</td>
<td>Information and Communication Technology</td>
</tr>
<tr>
<td>IDI</td>
<td>Information and Communication Technology Development Index</td>
</tr>
<tr>
<td>ILC</td>
<td>International Law Commission</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>ISIS</td>
<td>Institute for Science and International Security</td>
</tr>
<tr>
<td>ISP</td>
<td>Internet Service Provider</td>
</tr>
<tr>
<td>ITU</td>
<td>International Telecommunication Union</td>
</tr>
<tr>
<td>LAN</td>
<td>Local Area Network</td>
</tr>
<tr>
<td>NATO</td>
<td>North Atlantic Treaty Organisation</td>
</tr>
<tr>
<td>OECD</td>
<td>Organisation for Economic Co-operation and Development</td>
</tr>
<tr>
<td>P2P</td>
<td>Peer-to-Peer</td>
</tr>
<tr>
<td>PLC</td>
<td>Programmable Logic Controller</td>
</tr>
<tr>
<td>SQL</td>
<td>Structured Query Language</td>
</tr>
<tr>
<td>TCP</td>
<td>Transmission Control Protocol</td>
</tr>
<tr>
<td>UDP</td>
<td>User Datagram Protocol</td>
</tr>
<tr>
<td>UN</td>
<td>United Nations</td>
</tr>
<tr>
<td>UNESCO</td>
<td>United Nations Educational, Scientific and Cultural Organisation</td>
</tr>
<tr>
<td>US</td>
<td>United States</td>
</tr>
</tbody>
</table>
Acknowledgements

This thesis is the culmination of what I found to be an intellectually and psychologically challenging experience, yet one that was also extremely rewarding and valuable. I could not have done it alone, and I owe thanks to everyone who supported me along the way.

First, to my supervisors Associate Professors Kieran Tranter and Afshin Akhtarkhavari. They helped me to stay on track and provided me with valuable feedback, encouragement, and support throughout the project. Whether it was being compared to a mushroom ‘blossoming’ out of the earth, or being told to ‘just keep swimming’ – their feedback and advice was always greatly appreciated. Second, to the numerous people with whom I was fortunate enough to discuss various aspects of my work – whether here at Griffith University, at conferences, or at the University of Helsinki. All of these experiences helped with the development of my ideas and contributed to the overall shape of my thesis. Third, to my family and friends who have either supported me in my academic endeavours, or provided me with healthy distractions that put this project into perspective. Fourth, to those learned friends and fellow PhD students who helped proofread parts of my work. Finally, and most importantly, to my wife – without her support and encouragement I would not have been able to complete this project.

Chapter 1: Introduction

In international law, a classic example of the intersection between law and technology comes from the law of the sea. Prior to the modern twelve nautical mile limit of a state’s territorial sea, the so called cannon shot rule put this distance at three miles – the distance reflecting the technological capacity of cannons at the time. Despite debates about the origins of this rule and the exact technological capacity of cannons in the seventeenth and eighteenth centuries, the cannon shot rule reflects the basic idea that technology can shape how something is understood in law. In this instance, it helped shape the parameters of the legal space in which states can exercise their territorial sovereignty. More generally, the relationship between law and technology is often described like the race between the tortoise and the hare: technology is seen as moving fast whereas the law is slow and constantly needs to catch-up or it risks becoming outdated. While not all new technologies raise legal issues, particularly those technologies that make new things practicably possible do. For example, from the invention and development of bicycles and automobiles to Uber and driverless vehicles, new technologies have required updated laws to regulate new forms of transportation on roads and therefore have had an impact on the law.

The development of digital information and communication technologies (ICTs) in particular has also made a range of new behaviours and interactions possible for both state and non-state actors in and through cyberspace. In 2000 for instance, in the Australian state

---

1 On the origins of the rule, see Kent (1954) and Walker (1945). Wyndham Walker, for example, maintains that it is questionable whether any cannon at the time had a range of three miles. Walker (1945), p 210. Some go as far as maintaining that “[t]echnology gave birth to the Law of the Sea and continues to be a crucial factor in its development.” Picker (2001), p 168. Colin Picker writes how advances in maritime technologies that enabled early forms of economic globalisation were connected to the development of international law itself. For example, without these technologies, there would have been no need for the Dutch jurist Hugo Grotius to consider the freedom of the high seas (against the claims of dominion over the seas by the British), or for Francisco de Vitoria ‘to ponder the novel issues raised by the “discovery” of native peoples.’ See Picker (2001), pp 160-164.

2 Under the current law, pursuant to Article 3 of the United Nations Convention on the Law of the Sea, opened for signature 10 December 1982, [1994] ATS 31 (entered into force 16 November 1994), states have a right to establish a territorial sea of up to 12 nautical miles, and a state’s sovereignty extends to this area pursuant to Article 2.


4 According to Lyria Bennett Moses for instance, the most direct impact of technology on the law comes from the ‘capacity of new technology to enable new forms of conduct, including alteration of the means by which similar ends are achieved. The current state of technology limits in practice what actions we can perform, what objects we can create, and what relationships we can form.’ Bennett Moses (2007), p 245 (emphasis in original).

5 For example, on the impact of bicycle technologies on the law in the United States, see Brenner (2007), pp 34-41. On the impact of the introduction of automobile technologies in Australia, see Tranter (2005). For an overview of the legal impact of ‘disruptive’ technologies generally, see Katyal (2013).
of Queensland, an individual used a laptop to remotely obtain unauthorised access to the computer systems used to operate the local council’s sewage system. He altered data causing the system to malfunction, and this resulted in sewage escaping and causing environmental harm. On the other hand, in 2013 the blueprints for the Australian Security and Intelligence Organisation’s (ASIO) new headquarters were stolen from the computer system of a contractor involved in the construction process. While the identity of those responsible for accessing this system and obtaining this data are unknown, the source of the intrusion was traced to servers located in China. Similarly in 2015, the computer systems of Australia’s Bureau of Meteorology (BOM) were compromised by actors located in China in what was described as a ‘major attack’ that would cost millions of dollars to fix. Therefore, the development of digital ICTs enabling interactions in and through cyberspace have made a range of new things possible for both state and non-state actors, and this in turn has given rise to a number of legal issues.

This thesis is concerned with a particular intersection of international law and technology, namely the law on the use of force and cyber attacks. In this context it explores the thematic intersection of law, technology, and violence. Central to international law have always been efforts to regulate and limit interstate conflict and violence. In the modern context this concern is crystallised in the cornerstone provision of the United Nations (UN) Charter: the Article 2(4) prohibition on the use of force. This provision essentially prohibits states from engaging in particular forms of violence in their international relations. Outside specific legal rules prohibiting state behaviour however, international law is permissive in nature. As law operating between sovereign states and being dependent on their consent, it is regarded as permitting what it does not expressly prohibit. Accordingly, where states seek

---

9 Cyber attacks are commonly defined as referring to deliberate computer enabled actions used ‘to alter, disrupt, deceive, degrade, or destroy adversary computer systems or networks or the information and/or programs resident in or transiting these systems or networks.’ Owens et al (2009), pp 10-11. This thesis uses the term cyber attack descriptively, and therefore it is not to be confused with the notion of ‘attack’ that is used in the context of international humanitarian law for example. See Schmitt (2012a).
10 This principle stems from SS ‘Lotus’ (France v Turkey) (Judgment) [1927] PCIJ (series A) No 10 at 18 where the Permanent Court of International Justice maintained that:

International law governs relations between independent States. The rules of law binding upon States therefore emanate from their own free will as expressed in conventions or by usages generally accepted as expressing principles of law and established in order to regulate the relations between these co-existing independent communities or with a view to the achievement of common aims. Restrictions upon the independence of States cannot therefore be presumed.
to pursue their interests by less diplomatic means, for instance by obtaining unauthorised access to the computer systems and networks of another government and extracting information from those systems, there is a tension between what the law clearly prohibits (for example, those acts constituting a prohibited use of force) and especially those means below this threshold that are not covered by a specific legal rule (such as the non-intervention principle). This tension is particularly evident in relation to state activities in and through cyberspace because, while traditionally espionage for example is not prohibited by international law, the current technological context in which states operate both enables them to easily engage in a range of new activities and simultaneously renders them open to new vulnerabilities.

Writing in the years following the 11 September 2001 terrorist attacks, Rosalyn Higgins maintained that among the key issues in the law on the use of force are: ‘[w]hat sort of harm, against whom and where, constitutes an attack on a ‘State’ within the meaning of Article 2(4)?’ In the cyberspace context in particular, states can potentially from anywhere in the world cause new forms of harm against other states that might not involve bloody and destructive violence resembling traditional military offensives or the Al-Qaeda attacks on the United States (US). Therefore, obtaining unauthorised access to the blueprints of ASIO’s new headquarters from the computer of a private contractor, or compromising the integrity of the BOM’s computer systems may not be expressly prohibited by international law nor constitute the type of harmful behaviour that the prohibition on the use of force was originally concerned with in 1945. However, these behaviours in and through cyberspace reinvigorate questions about what types of state activities are expressly prohibited by the law in the twenty-first century. As such, questions arise again about the types of harmful interactions that are or should be prohibited, what harm looks like in a world of increasingly ICT dependent states, and even what the state as an entity capable of being subject to harm looks like in this world. These are among the key questions that this thesis seeks to explore.

Within the law on the use of force, the primary focus of this thesis is on cyber attacks and the threshold distinction between what amounts to ‘force’ within Article 2(4) and the

---

This principle has been subject to criticism. See, for example, Crawford (2012), p 42, note 25. See also Koskenniemi (2006), pp 255-258.
11 See, for example, Demarest (1996), pp 338-339.
12 Higgins (2009), p 268. Writing in the years following the 11 September 2001 terrorist attacks in the United States, Higgins connects these questions to terrorism in particular.
measures below this threshold that are considered to breach the non-intervention principle alone. Therefore, it is concerned with the law on the use of force in a narrow sense. The issues of threats of force; the requirement that uses of force (and threats of such) must occur in the ‘international relations’ of states; and the need for any such force to be against the territorial integrity of another state or in any way that is inconsistent with the general purposes of the UN Charter, are of secondary concern. Similarly, this thesis is not concerned with the international legal responses permitted against cyber attacks. These include, for example, non-forceful countermeasures that are used to ensure another state’s compliance with an international obligation that they have breached. It is also not concerned with cyber attacks rising to the level of an armed attack against which states are permitted to use force in self-defence pursuant to Article 51. Related issues such as, whether states can respond to cyber attacks with cyber attacks, or whether traditional military force can be used against cyber attacks in self-defence, are also not the focus. Instead, within the general area of law on the use of force, this thesis is primarily concerned with the threshold distinction between what amounts to ‘force’ within Article 2(4) and what does not. As such, the non-intervention principle is considered to the degree that it is relevant in distinguishing between what is understood to constitute ‘force’ and what falls below this threshold in relation to cyber attacks specifically. Accordingly, this thesis is mainly concerned with the threshold distinction between the non-use of force principle and the non-intervention principle.

Often the term ‘incidents short of war’ are used to describe those measures amounting to a use of force but which are considered to fall below the armed attack threshold. Yoram Dinstein for example writes that:

Incidents involving the use of force, without reaching the threshold of war, occur quite often in the relations between States. Border patrols of neighbouring countries may exchange fire; naval units may torpedo vessels flying another flag; interceptor planes may shoot down aircraft belonging to another State, and so forth.

---

13 Pursuant to Article 51 of the UN Charter, states retain their inherent right to self-defence following an armed attack. As will be discussed in chapter 4, while an armed attack always involves a use of force, not all uses of force rise to the level of an armed attack.

14 Dinstein (2001), p 11. For Dinstein, ‘[w]ar is a hostile interaction between two or more States, either in a technical or in a material sense. War in the technical sense is a formal status produced by a declaration of war. War in the material sense is generated by actual use of armed force, which must be comprehensive on the part of at least one party to the conflict.’ Dinstein (2001), p 15.
On the other hand, economic coercion for example is not considered a form of ‘force’ for the purposes of Article 2(4), and falls below this threshold into the realm of the non-intervention principle instead.\(^{15}\) In this thesis it is argued that through the threshold distinction between the non-use of force and non-intervention principles, international law defines the boundaries of what is conceptualised as interstate violence. Consider for instance the above incidents which involve the use of force according to Dinstein. Whether it is the members of the armed forces of one state inflicting harm to human soldiers of another state through kinetic weapons, or the launching of missiles or torpedoes that cause physical damage to the hulls of planes or naval vessels; in each instance the incidents involve a use of force understood as a particular form of violence involving injury or death to human beings or damage or destruction of physical objects. As such, it is argued that the dominant understanding of what constitutes a use of force under international law embodies a particular conceptualisation of violence.\(^{16}\)

Cyber attacks are challenging this conceptualisation of violence. As will be illustrated when considering the cyber attacks against Estonia in 2007 and the Stuxnet incident, especially where cyber attacks do not result in material effects they largely fall outside the law’s conception of violence that is embodied in Article 2(4). However, where a cyber attack has material effects the law has the ability to recognise it as a form of violence within the ambit of Article 2(4). It is argued that the reason for the conceptual challenge to how interstate violence is understood, which is manifested in the use of cyber attacks, is not simply a result of new things becoming possible due to technological advances. Instead, it is argued that the reasons are ontological. Generally ontology refers to the study of what is said to exist. In this thesis ontology is examined in the context of what exists in the eyes of the law and therefore what the law is capable of recognising as real.\(^{17}\) As will be demonstrated, the law subscribes to a particular worldview in which violence is understood in inherently


\(^{16}\) As will be shown in chapter 4 in particular, this is evident in how the notion of force within Article 2(4) is interpreted. Tom Farer for instance writes that Article 2(4) is not concerned with economic coercion as it is ‘concerned with violence, with military force’. Farer (1985), p 410. Yoram Dinstein in turn writes that ‘the term ‘force’ in Article 2(4) must denote violence. It does not matter what specific means – kinetic or electronic – are used to bring it about, but the end result must be that violence occurs or is threatened.’ Dinstein (2011), p 88.

\(^{17}\) This is different to how the notion of ‘law’s ontology’ is used, for example, in debates in legal theory about what the essence of the law is and the conditions for its existence. For these debates, see Amselek and MacCormick (1991). See also Melkevik (2013), pp 230-232. As will be discussed below, to both highlight and critique the law’s ontological limitations, this thesis draws on a theory that is ontologically committed to an informational ontology. This means that it adopts the view that everything can be seen as information structures and that these information structures exist. See Floridi (2006), pp 26-31.
anthropocentric and materialist terms as requiring harm to human beings or damage to physical objects. Therefore, it is argued that the law’s inability to recognise cyber attacks with non-material effects, such as damage to data or the disruption of information systems, as a form of violence, is a result of the law’s ontological constraints. This is evident in its limited capacity to recognise cyber attacks with non-material effects as a form of ‘force’ within Article 2(4).

Where cyber attacks do not result in material effects and fall below the use of force threshold, they are often considered as potential breaches of the non-intervention principle instead. While the non-intervention principle was classically concerned with ‘forceful intervention’, in its modern form it is understood to prohibit states from using coercive measures not involving military force. In relation to cyber attacks in particular, as will be demonstrated in the review of existing literature on cyber attacks and the non-use of force and non-intervention principles, the non-intervention principle is used to capture those cyber attacks that fall below the use of force threshold that do not result in material effects.

It is argued that in doing so, cyber attacks below the use of force threshold are depicted as a form of non-violence. As a result, cyber attacks with non-material effects largely fall outside the use of force principle – the cornerstone provision of the UN Charter that seeks to limit international violence – into what the law conceptualises as forms of non-violence only affecting the ‘personality of the state’. This is illustrated by the 2007 cyber attacks against Estonia which are generally not considered to have constituted a use of force under existing law, instead amounting to a breach of the non-intervention principle alone. In contrast, as will be illustrated by the Stuxnet incident, where a cyber attack results in material damage to physical objects such as nuclear centrifuges, the law is more readily able to recognise it as a form of violence prohibited by Article 2(4).

18 Lassa Oppenheim for example defined it as ‘forcible or dictatorial interference by a State in the affairs of another State, calculated to impose certain conduct or consequences on that other State.’ Watts and Jennings (1992), p 430 cited in Harris (2010), p 743.
19 See part one of chapter 4. This distinction is made in the Declaration on Principles of International Law Concerning Friendly Relations and Co-operation among States in Accordance with the Charter of the United Nations (adopted by the UN General Assembly on 24 October 1970, UN Doc A/RES/2625(XXV)), and by the International Court of Justice in Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v United States of America) (Merits) (1986) ICJ Reports 14 at 108 (para 205).
20 See part two of chapter 4. Heather Harrison Dinniss for instance writes that even where a cyber attack does not rise to the level of a use of force, it does not mean it is permissible as it is likely that it will be considered an unlawful intervention. Dinniss (2012), p 74. Similarly, Marco Roscini concludes that cyber attacks which are not destructive or severely disruptive are not uses of force but ‘may be unlawful interventions in the internal affairs of other states’. Roscini (2014), p 115.
Accordingly, while technology in the context of the seventeenth and eighteenth century cannon helped shape the law of the sea, technology in the context of cyber attacks is both shaping and challenging how the notion of violence is understood through international law on the use of force. This thesis argues however, that the reasons for this challenge are not simply technological but ontological. The harm that cyber attacks cause, particularly where there is no injury to human beings or damage to physical objects and the effects are mainly informational, is at odds with the anthropocentric and materialist conception of violence that is embodied in existing law. Given the increased ways in which states are becoming more and more dependent on ICTs as ‘information societies’, even cyber attacks without material effects can harm states in new ways that are not adequately accounted for by existing law. As such, cyber attacks highlight the need to rethink the notion of violence.

Violence has always been central to international law. From the Thirty Years’ War and the consequent treaties of Westphalia in 1648 cementing the early foundations of the modern state; to the Geneva and Hague Conventions\(^{21}\) that sought to limit the violence in warfare and continue to provide the basis for modern international humanitarian law; and the institutional efforts to limit the outbreak of interstate war following World War I and II that are now embodied in the UN Charter\(^{22}\) – rules regulating the violence in warfare and the outbreak of violent warfare have had a central position in the development of international law. The modern state has also played a crucial role in these developments. As the primary subject of international law and the dominant organisational structure in the international system,\(^{23}\) the state is the sole entity with a monopoly of violence internally within its

\(^{21}\) Among the original Geneva Conventions was, for example, the *Geneva Convention for the Amelioration of the Condition of the Wounded in Armies in the Field*, 22 August 1864, available at https://www.icrc.org/ihl/INTRO/120?OpenDocument. This has been replaced by the *Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armies in the Field*, opened for signature 27 July 1929, [1931] ATS 6 (entered into force 19 June 1931). As to the original Hague Conventions, see for instance the *International Convention with Respect to the Laws and Customs of War on Land*, opened for signature 29 July 1899, [1901] ATS 131 (entered into force 4 September 1900).

\(^{22}\) According to Antonio Cassese for example, ‘[o]ne of the major reactions to the devastations of the Second World War and the unfettered recourse to violence marking those dark years was the keen desire to set up a world organization that would be capable of preventing ‘the scourge of war’ and peacefully settling all major disputes between States.’ Cassese (2005), p 40.

\(^{23}\) Christoph Schreuer for example writes that the sovereign state is the prototypical international actor and the ‘universal standard’ in international law, and that:

Contemporary international law presupposes this structure of co-equal sovereign States. The international community’s constitutive set-up is dominated by it. The classical sources of international law depend on the interaction of States in the form of treaties and customary law. Diplomatic relations are conducted between States. Official arenas, like international organizations and international courts, are largely reserved to States.
terrestrial borders and internationally as the entity legitimately capable of engaging in warfare. International law on the use of force is also premised on these assumptions of what the state is, and on certain assumptions about what constitutes a form of violence against the state. Violence in this context traditionally involves the armed forces of one state engaging in conflicts on physical territory with kinetic weapons against the armed forces of another state. In contrast, cyber attacks by states against other states can originate from across the globe; they can be launched with a degree of anonymity; they may not breach the territorial integrity of a state nor manifest in material effects within a state; and they may not inflict harm through the usual instruments of violence that are associated with uses of military force. As an example of the new ways in which states can be harmed, and in highlighting the changing nature of violence, it is argued that the use of cyber attacks against states also invites a rethinking of the state as the entity subject to violence. As will be shown, especially because states are increasingly dependent on ICTs for their proper functioning, they can also be harmed by cyber attacks with non-material effects. This means that cyber attacks that disrupt the functioning of states, even where they only affect information or disrupt the operation of information systems, amount to what will be described as a form of ‘informational violence’ against the state.

An Overview of Information Ethics

Returning then to the questions posed earlier about the types of harmful interactions that are or should be prohibited, what harm looks like in a world of increasingly ICT dependent states, and even what the state as an entity capable of being subject to harm looks like in this world. To explore these questions, this thesis draws on Luciano Floridi’s information ethics.25


24 See, for example, Thomson (1995), pp 219-228. See also chapter 3.

25 Floridi’s information ethics was originally developed in Floridi (1999) and most recently and comprehensively in Floridi (2013). Others that have drawn on Floridi’s information ethics in relation to international law and cyber warfare include: Taddeo (2012); Taddeo (2016); Pagallo (2015a); Durante (2014). As to Floridi’s information ethics and law more generally, Dan Burk for example provides a ‘test drive’ in the application of information ethics to the legal landscape of data representations, see Burk (2008). He maintains that information ethics can be applied to legal doctrine but not in its current form (he maintain that it first needs to give guidance as to who information belongs to) Burk (2008), p 146. He does note however, that the most compelling cases for its application arise within the legal context of cyberspace – in this context, its framework of ethical principles ‘has clear implications for legal doctrine. Law as a formalized and applied set of ethical practices is ultimately grounded in some framework of guiding principles; information ethics aspires to provide such principles.’ Burk (2008), p 135. Others, such as Timothy Colburn and Gary Shute, consider information ethics and the law in the computer science (opposed to legal) sense, see Colburn and Shute (2010). Massimo
While chapter 2 will describe information ethics in more detail, it is warranted to provide a basic overview here. Information ethics can be best described as a form of environmental ethics. Like environmental ethics, which Floridi describes as ‘biocentric’ frameworks that are concerned with biological entities and ecosystems, and the intrinsic value of life, information ethics is also concerned with the wellbeing of the recipient (opposed to the agent) of any action. As such, it can be described as:

an ecological ethics that … replaces biocentrism with ontocentrism. It suggests that there is something even more elemental than life, namely being – that is, the existence and flourishing of all entities and their global environment – and something even more fundamental than suffering, namely entropy.

Instead of a concern with the wellbeing of the biosphere, information ethics is concerned with the wellbeing of the ‘infosphere’. The infosphere refers to ‘the environment constituted by the totality of information entities’. For methodological purposes information ethics therefore advocates the adoption of an informational ontology which provides a minimum common denominator through which all entities can be seen in similar terms.

By adopting an informational ontology, that is, by adopting a perspective from which all entities can be viewed in terms of their information structures, all entities can be seen as information entities. This means that ‘not only all persons, their cultivation, wellbeing, and social interactions, not only animals, plants, and their proper natural life, but also anything that exists, from paintings and books to stars and stones’ can be viewed as information entities that collectively constitute the infosphere. Information ethics also suggests that everything should have a basic degree of moral value pursuant to the ontological equality principle.

As a result of the ontological equality principle, every information entity, ‘simply for the fact of being what it is, enjoys a minimal, initial, overridable, equal right to exist and

---

26 Floridi (2010a), p 111.
27 Floridi (2010a), p 112.
28 Floridi (1999), p 44.
develop in a way which is appropriate to its nature." In this context, being or existence is seen as inherently good whereas entropy is regarded as evil. Floridi adopts a very particular definition of entropy that is different to the use of the term in thermodynamics for example. In his use of the term, it essentially refers to any degradation of being, such as the destruction or corruption of information entities.

To guide the behaviour of responsible and caring agents within the infosphere, information ethics provides basic rules that aim to respect and promote the wellbeing of the entire infosphere. Information ethics therefore provides an environmental approach to thinking about what is good for the infosphere and, in doing so, it offers an approach that advocates respect for both the material and non-material world.

**Research Question and Methodology**

Accordingly, in light of this theoretical framework and the aforementioned questions that this thesis seeks to explore, the primary research question guiding this research can be stated as:

How can the notion of violence embodied in international law on the use of force be reconceptualised through an informational approach to account for the law’s ontological constraints in relation to the non-material effects of cyber attacks?

This question is primarily examined through case studies. The methods used in the case studies involve doctrinal and archival research. Archival research is used to gather and triangulate data about the cyber attack incidents considered in each case study. Doctrinal research is used to first describe the law as it relates to the threshold distinction between the

---

34 Floridi (2013), p 71. These rules are: 0) entropy ought not to be caused in the infosphere (null law); 1) entropy ought to be prevented in the infosphere; 2) entropy ought to be removed from the infosphere; and 3) the flourishing of informational entities as well as of the whole infosphere ought to be promoted by preserving, cultivating and enriching their wellbeing. Others have considered these rules in relation to just war principles, see Taddeo (2016), pp 221-222; Fugallo (2015a), pp 416-419.
36 According to Robert Yin, case studies are useful when considering ‘how’ or ‘why’ questions in relation to contemporary events that the researcher has little control over. They allow researchers to examine the ‘holistic and meaningful characteristics of real-life events’ in order to make sense of ‘complex social phenomena’. Yin (2009), pp 2-4.
37 Archival research involves ‘locating, evaluating, and systematic interpretation and analysis of sources found in archives.’ Corti (2003), p 20. The primary sources used in this thesis include, for example: media and technical reports on cyber attacks, resolutions from various organs of the United Nations, and primary legal and related contextual material.
non-use of force and non-intervention principles (chapter 4); and second to describe how the law is understood to apply to the cyber attack incidents that are considered in each case study (chapters 5 and 6). Using the data derived from these research methods, the case studies will provide an in-depth account of the events, the technical details about the cyber attacks, and how the law is understood to apply to each incident under consideration. Additionally, drawing on the theoretical framework of information ethics that is described in chapter 2, the case studies will undertake a critical and analytical study of the law as it relates to the cyber attack incidents that are examined. In doing so, the case studies will be used to illustrate the limitations of existing law (that is, the law’s ontological constraints) and examine how information ethics offers an approach through which these constraints can be overcome.

The two case studies that were chosen are the 2007 cyber attacks against Estonia, and the Stuxnet incident involving Iran. These case studies were chosen for two primary reasons. First, because they involve cyber attacks believed to have been supported or conducted by state actors against other states that were sufficiently serious to raise questions of international law in relation to the threshold distinction between the non-use of force and non-intervention principles. As such, these incidents also highlight how the state as the entity subject to violence can be harmed through cyber attacks. As will be shown in chapter 5, in much of the secondary literature on the law, the cyber attacks against Estonia are not considered to have crossed the use of force threshold. In contrast however, as will be shown in chapter 6, the Stuxnet incident is more widely considered to have crossed the use of force threshold. Together these case studies illustrate the boundaries of the threshold distinction.

---

38 Doctrinal research is a form of qualitative legal research that involves asking what the law is in a particular area by collecting and analysing relevant primary and secondary sources of law. Dobinson and Johns (2007), pp 18-19. On traditional doctrinal research methods in international law, see Hall (2007). For an overview of this and other methods in international law, see Ratner and Slaughter (1999), pp 291-295. For a critical account of the notion of legal ‘style’ as opposed to legal ‘method’, see Koskenniemi (1999), pp 352-354.

39 The cyber attacks against Georgia in 2008 were excluded after an initial screening for a number of reasons. First, the Georgia incident bears similar characteristics to the Estonia incident that occurred the prior year. For example, both were similar in terms of the technical methods used in the attacks. Also similar to the Estonia incident, the cyber attacks against Georgia are believed to have been carried out by non-state actors with potentially some degree of support from, or involvement by, Russian state officials. The second reason comes from key differences between the two incidents. In contrast to the Estonia incident, the cyber attacks against Georgia largely occurred in conjunction with a traditional military offensive and, as such, are considered to have occurred within an armed conflict. In international law, this triggers the operation of international humanitarian law. Therefore, the Georgia incident is useful for considering the issues surrounding the operation of international humanitarian law in relation to cyber attacks, but that area of law is not the focus here. As a result, the cyber attacks against Estonia were deemed more appropriate to consider the law on the use of force, and also because the attacks were not accompanied by a more traditional military offensive that would be less controversially considered a use of force under existing law. On the Georgia incident, see Tikk et al (2010), pp 66-90.
between the non-use of force and non-interference principles in relation to cyber attacks. This demonstrates both what the law is capable of recognising as ‘force’ in relation to cyber attacks and what it is not. Further, it provides an opportunity to illustrate how an informational approach can be used to overcome the law’s shortcomings in this context. The second reason why these case studies were chosen is practical. Both of these incidents were widely reported on in the media; Stuxnet in particular was thoroughly examined by cyber security experts and therefore technical reports about its design are available; and both incidents are widely discussed in secondary literature on international law in relation to cyber attacks. As such, there is sufficient data available on both incidents to develop an in-depth account of the events that occurred, the technical details of the attacks, and the secondary literature that examines the legal issues surrounding the incidents.

Overall, this thesis argues the law on the use of force embodies an ontologically constrained view of violence. Violence is seen in anthropocentric and material terms, as requiring damage or destruction of physical property, or injury or death to human beings. As a result, the ‘harm’ associated with cyber attacks without material effects – essentially only affecting information – largely falls outside the law’s existing conceptualisation of violence and consequently the legal doctrines through which interstate violence is regulated. In an effort to overcome these ontological constraints, Floridi’s information ethics will be drawn on to reconceptualise the notion of violence and the state as the entity subject to violence. Consequently, it is argued that through an informational approach, the law’s ontological constraints can be reconfigured, meaning that non-material forms of ‘informational violence’ can be recognised. This in turn offers a means through which cyber attacks without material effects that currently escape the law’s conceptualisation of violence become a form of violence capable of harming the state entity. As such, given the law’s central concern with containing violence and limiting harmful interactions between states, informational violence too can be brought into the law’s conceptual containment.

**Overview of Thesis**

As mentioned, chapter 2 will begin by describing Floridi’s information ethics. By examining the aforementioned framework, it will provide the conceptual foundations on which this thesis will draw on to provide a critique of the anthropocentric and materialist conception of violence inherent in existing law on the use of force. Further, it provides the basis for the
adoption of an informational approach through which, it is argued, the law’s ontological constraints can be overcome.

Chapter 3 explores international law and the containment of violence. It begins by exploring the ways in which international law has traditionally sought to regulate various flows of information globally, including information flows which are deemed harmful under international law. It then moves to consider international law’s historical concern with limiting the outbreak of interstate conflict and violence, in what is described as the law’s containment of violence. Against the traditional account of the law’s containment of violence, this chapter will then consider the novel nature of cyber warfare. It is argued that there is an ontological gap between traditional or kinetic warfare and cyberwarfare. While cyberwarfare can involve death and destruction like traditional warfare, more often it lacks these characteristics and involves damage or disruption to information and networks. Consequently, the law embodies an ontologically constrained view of violence that lacks the ability to recognise the new forms of harm more commonly associated with cyberwarfare (how this manifests in legal doctrine on the use of force will be examined in chapter 4). Finally, this chapter adopts an informational approach to offer a reconceptualisation of the state entity and the notion of violence. The state entity is described as an information system that increasingly interacts with other entities, and violence is described through the notion of entropy as the degradation of the state entity.

Chapter 4 then considers the threshold distinction between the non-use of force and non-intervention principles. In this context it is argued that the law embodies an ontologically constrained view of violence. This is particularly evident in existing international legal scholarship on the use of force in relation to cyber attacks, as cyber attacks with material effects are deemed a form of violence within the non-use of force principle, whereas cyber attacks with non-material effects are considered through the non-intervention principle and depicted as a form of non-violence. It is then argued that an informational approach offers a means through which to consider cyber attacks also as a form of informational violence that is capable of undermining the integrity and functioning of the state entity as an information system.

Chapter 5 provides the first of two case studies. It considers the 2007 cyber attacks against Estonia. In April and May of 2007, Estonia was subject to large scale Distributed
Denial of Service (DDoS) attacks lasting over three weeks in total and which impacted on the functioning of its government and civil society. In this thesis, the Estonia incident is used to demonstrate the law’s ontologically constrained view of violence highlighted in chapter 4. Particularly as the cyber attacks did not result in material damage, the incident is widely considered not to have constituted a use of force and is at most deemed to have breached the non-intervention principle. It is argued that as a result of the law’s ontological constraints, the cyber attacks against Estonia largely fall outside of the law’s conceptualisation of violence as the law lacks the capacity to recognise forms of informational violence. Consequently, drawing on the informational approach developed in preceding chapters, an informational analysis of the incident is used to demonstrate that it offers a means to overcome the law’s ontological constraints and recognise a broader spectrum of violence. Therefore, by viewing the Estonian entity as an information system dependent on ICTs for its functioning, the cyber attacks can be seen as a form of informational violence causing entropy. In particular, the attacks undermined the Estonian entity’s ability to interact, its autonomy, and its ability to care for and protect the entities within its region of the infosphere.

Chapter 6 then considers the Stuxnet incident. The Stuxnet cyber attack against Iran’s uranium enrichment facility in Natanz was discovered in 2010. It is believed to have been a joint US and Israeli effort to undermine Iran’s uranium enrichment program and, unlike the Estonia incident, Stuxnet is believed to have caused material damage to nuclear centrifuges. In this thesis Stuxnet is used to illustrate that the law has the capacity to recognise cyber attacks with material effects as a form of violence. This is evident in the dominant view that it constituted a use of force particularly as it caused material damage. However, it is argued that, as a result of its ontological constraints, the law only provides a one-dimensional account of violence. This is evident in existing legal analyses of Stuxnet in which its material effects are emphasised whereas its non-material effects or forms of informational violence are not adequately accounted for. It is argued that, by adopting an informational approach, in addition to the material damage to centrifuges that Stuxnet caused, the various non-material ways in which it undermined and degraded the integrity of thousands of entities within Iran’s region of the infosphere and within the Natanz system can also be considered. Therefore, it is argued that an informational approach offers a means not simply to recognise a broader spectrum of violence, but it also provides a deeper account of violence.
To conclude this thesis, chapter 7 first provides an overview of the informational approach developed in the preceding chapters. It then discusses the contribution of this thesis to information ethics as a field. It also examines the wider relationship between law and informational violence, and how an informational approach can contribute to the development of international law on the use of force in particular. Finally, in an effort to outline potential sites for future research, it considers some of the conceptual implications of this approach for international law more generally.
Chapter 2: Information Ethics

Introduction

This chapter describes Luciano Floridi’s information ethics. This conceptual framework will be used in this thesis to develop an informational approach to cyber attacks and the law on the use of force. This chapter consists of two sections. The first section locates Floridi’s information ethics within the philosophy of technology. It outlines what Floridi describes to be the wider philosophical and technological transformations and challenges that give rise to the need for new conceptual toolkits such as information ethics. The second section then explores the key principles and concepts of information ethics, as well as the criticisms that have been levelled against it. These concepts, namely the ontological equality principle, the infosphere, and entropy, will then be drawn upon to build an informational approach in subsequent chapters.

Section 1: The Philosophies of Technology and Information

1.1 Philosophy of Technology

The tension between nature and technology and their relationship to humans is a prominent theme in the philosophy of technology. The roots of these concerns can be traced to ancient Greek philosophy and distinctions between what is considered part of nature (the notion of physis) and those artefacts that are produced by humans (the notion of technē). The Greeks saw an inherent essence in the idea of an artefact that then comes into existence when man produces it, and as such, humans were not regarded as masters of nature but merely bringing the natural world into fruition. In contrast, modern views of technology and the relationship between humans and technological artefacts, see technology not as a part of nature but in instrumental terms. Indeed, modernity is pervaded by an inherently instrumentalist philosophy of technology. Technology from an instrumental view is conceptualised as tools or machines – artefacts are made by humans but they are distinct from nature and can be used for any purpose. Thus technology is regarded as value-neutral and something under the

---

control of humans through which nature can be exploited and dominated.\textsuperscript{4} From this view, the only value that technology embodies is the value of formal efficiency – finding the most efficient way of realising pre-existing values.\textsuperscript{5} This view of technology also aligns with the modern belief in progress through technological advancement aimed at the fulfilment of human needs.\textsuperscript{6} However, much of the perceived promise of technology and the benefits of its advancement became undermined by the realisation that technology could not just be helpful, but also extremely harmful. This was seen particularly after the deployment of nuclear weapons in World War II, and as the ecological side effects of technology became evident in second half of the twentieth century.\textsuperscript{7} Therefore, while technology could be used to achieve any human ends, the scientific rationality associated with modernity meant that there was a ‘strange aimlessness’ as to what those ends were.\textsuperscript{8}

More critical theories of technology emerged particularly in the second half of the twentieth century that described technology and its relationship to the world differently. Various approaches addressed the earlier view of technology as seemingly neutral, instead demonstrating the socially constructed nature of technologies,\textsuperscript{9} the politics technologies embody,\textsuperscript{10} and challenging the perceived human control over technological development.\textsuperscript{11} Critical theories of technology often perceive the concept of technology more broadly as an environment or as more complex systems,\textsuperscript{12} opposed to merely a collection of tools and machines.\textsuperscript{13} As part of the environment in which humans live, technology shapes humans and their interactions\textsuperscript{14} and provides ‘frameworks for ways of life.’\textsuperscript{15} These views mark a shift from merely an instrumental view of technology as tools under human control used for

\textsuperscript{4} Feenberg (2006), p 9. This is in contrast to what are often described as ‘substantivistic’ views on technology that see technology not as value neutral but embodying power and domination. See Feenberg (2006), pp 11-12. See also Mitcham and Waelbers (2009), p 371. For instance, Martin Heidegger’s account of technology is often classed in this way, see Van Den Eede (2015), p 151; Feenberg (2006), p 12.
\textsuperscript{5} Feenberg (2006), p 11.
\textsuperscript{6} Feenberg (2006), pp 9-11.
\textsuperscript{7} Dusek (2009), pp 132-133.
\textsuperscript{8} Feenberg (2006), p 9.
\textsuperscript{9} On the ‘social construction of technology’, see, for example, De Vries (2005), pp 78-79; Dusek (2006), pp 203-205.
\textsuperscript{10} Winner (1980).
\textsuperscript{11} Mitcham and Waelbers (2009), p 373.
\textsuperscript{12} See Dusek (2006), pp 32-33.
\textsuperscript{13} Feenberg (2009), p 148.
\textsuperscript{14} Feenberg (2009), p 148.
\textsuperscript{15} Feenberg (2006), p 14.
whatever means they choose, to instead considering technology as an evolving and wider environmental force that both shapes the socio-political order and is itself shaped by it.\textsuperscript{16}

The philosophy of technology – that is, the conceptual framework through which technology and its relationship to humans and the natural world is understood – is particularly important in helping make sense of modern ‘information societies’ pervaded by technology. As part of the Europe 2020 initiatives in connection with the European Commission’s ‘Digital Agenda’ for Europe, a group of academics from a range of disciplines from law to neuroscience reflected on the wider political, social and policy related impacts of information and communication technologies (ICTs).\textsuperscript{17} The project was entitled \textit{The Onlife Initiative: concept reengineering for rethinking societal concerns in the digital transition} (the Onlife Initiative’) and resulted in the publication of \textit{The Onlife Manifesto: Being Human in a Hyperconnected Era} (the Onlife Manifesto).\textsuperscript{18} Its authors argue that the transformations associated with ICTs and their impact on the human condition is challenging the philosophical foundations of existing conceptual toolkits.\textsuperscript{19} They maintain that ICTs are not simply tools but environmental forces that are impacting on:

1. our self-conception (who we are);
2. our mutual interactions (how we socialise);
3. our conception of reality (our metaphysics); and
4. our interactions with reality (our agency).\textsuperscript{20}

The authors attribute the reasons for this impact of ICTs on at least four major transformations:

a. the blurring of the distinction between reality and virtuality;
b. the blurring of the distinction between human, machine and nature;
c. the reversal from information scarcity to information abundance; and
d. the shift from the primacy of stand-alone things, properties, and binary relations, to the primacy of interactions, processes and networks.\textsuperscript{21}

\textsuperscript{16} Feenberg (2009), pp 146-148.
\textsuperscript{17} Floridi (2015b), pp xi-xiv.
\textsuperscript{18} Floridi (2015b), p 1; The Onlife Initiative (2015).
\textsuperscript{19} Floridi (2015b), pp 2-3.
\textsuperscript{20} Floridi (2015b), p 2.
These transformations, the authors maintain, challenge some of the very assumptions of modernity. For example, they argue that policymaking is still largely underpinned by various ‘political, social, legal, scientific and economic concepts’ that remain ‘deeply anchored in questionable assumptions about modernity.’ These include the view of the inherent distinction between technology and nature, the attribution of ethical responsibility mainly to rational humans as opposed to technological artefacts, and the pervasiveness of various mechanical metaphors, like the notion of control, within modern worldviews, structures and forms of political organisation. They argue that the development of ICTs is challenging these assumptions because the distinction between the artificial and natural is being blurred, ICTs can increasingly operate autonomously inviting notions of distributed responsibility, and ICTs destabilise modernity’s mechanical worldviews and metaphors by enabling new forms of political organisation. The authors of the Onlife Initiative maintain that especially due to these transformations, existing conceptual frameworks need to be updated in order to better understand the various problems related to ICTs and to be better equipped to solving them satisfactorily. Therefore, in light of these transformations and wider impact of ICTs, Floridi’s philosophy of information and information ethics seek to provide a conceptual framework to address the ethical challenges associated with ICTs.

1.2 Luciano Floridi’s Philosophy of Information

Since the late 1990s, various aspects of a philosophy of technology based on information have been developed in the work of Luciano Floridi. Given the central role of information in the digital or ‘information age’, Floridi has sought to develop a set of conceptual tools

26 Floridi (2010c), pp 402-403. Floridi’s major works, many of which are based on articles he has previously published, currently include: Floridi (2010a); Floridi (2011); Floridi (2013); Floridi (2014).
27 Hilmi Demir maintains that the notion of the information age is traceable to developments in 1940s and generally refers to the ‘age when computers have become an essential part of our daily lives.’ It is a time ‘dominated by information and communication technologies.’ Demir (2010), p 1. Terrell Bynum uses the term to refer to ‘technical and scientific developments in the 1940s that enabled a remarkable “explosion” of new products and innovations in the 1950s and beyond.’ It was then the exponential growth of the social and ethical issues caused by these developments, warranting the use of the notion of an ‘information revolution.’ See Bynum (2010), p 420.
through a philosophy of information. The basic premise of his philosophy, building on contributions by earlier figures such as Claude Shannon and Norbert Wiener, is that everything in the world is made up of information. Hence the entire universe and all of reality, given a particular level of abstraction, can be regarded as made up of information structures. Information in this context is not understood semantically – as news or content for instance – but as ‘equivalent to patterns or entities in the world.’ Within Floridi’s philosophy of information, information is therefore regarded as ‘something as fundamental and significant as knowledge, being, validity, truth, meaning, mind, or good and evil’ and hence worth philosophical investigation. However, it is also a concept through which these concepts can be expressed and investigated philosophically. Thus given the ways in which it aims to investigate information in all of its forms and at all stages in the information lifecycle, Floridi seeks to provide his philosophy of information as the philosophy of information, and as an entirely new paradigm through which to understand the world.

28 Floridi defines his philosophy of information as ‘the philosophical field concerned with (a) the critical investigation of the conceptual nature and basic principles of information, including its dynamics, utilization, and sciences; and (b) the elaboration and application of information-theoretic and computational methodologies to philosophical problems.’ Floridi (2011), p 14. As Patrick Allo notes, it is not simply ‘about the concepts of information and computation, it is also concerned with applications of informational and computational methods and models to philosophical problems’. See Allo (2010), p 248.

29 See Illari (2012), pp 12-18. For Norbert Wiener, physical objects and processes were made up of ‘patterns of information encoded with an ever-changing flux of matter-energy’ and any irreversible loss of physical information constituted thermodynamic entropy. See Bueno (2010), p 424. He also viewed humans as ‘fundamentally informational’ – that is, as patterns of information, and the flourishing of a person, which depended on information processing, as the overall purpose of life. Bueno (2010), pp 426-427.

30 According to Patrick Allo, while there had clearly been an ‘informational turn’ in philosophy, ‘Floridi gave that turn a more radical twist by claiming that taking the informational turn means redefining philosophy.’ Allo (2010), p 247.

31 The level of abstraction is essentially the perspective or degree of abstraction used when perceiving something. This will be explained in more depth below.

32 This is Floridi’s notion of ‘informational structural realism’ – the idea that the nature of reality is ultimately informational and can be regarded as ‘mind-independent and constituted by structural objects that are neither substantial nor material (they might well be, but we have no need to suppose them to be so) but informational.’ Floridi (2008a), p 241. See also Bynum (2010), p 432-433; Gillies (2010), p 20; Brey (2008), p 112.

33 Floridi (2010a), p 110.

34 Floridi (2013), p xii.

35 Floridi (2013), p xii.

36 Bynum describes Floridi’s philosophy of information as an ambitious project aimed at creating a ‘new philosophical paradigm’ founded on the concept of information, see Bynum (2010), p 431. According to Hilmi Demir, Floridi has in many ways defined the modern field of philosophy of information. Demir writes that: Floridi’s framework not only defines the content and the boundaries of Philosophy of Information as a field of inquiry but also provides novel approaches and ideas for a wide range of philosophical issues, ranging from Ethics to Logic (his Information Ethics and Informational Logic), from Ontology to Epistemology (his Informational Epistemology and Informational Metaphysics), from Semantics to Philosophy of Mind.

Demir (2010), p 3.
1.2.1 The fourth revolution and the ‘reontologisation’ of the infosphere

Accordingly, Floridi’s philosophy of technology is based on his philosophy of information. His argument, much like that in the Onlife Manifesto, is that ICTs have brought about radical conceptual challenges. These challenges are connected to what he describes as the ‘fourth revolution’ in human self-understanding. The origins of this revolution can be traced to the ideas of Alan Turing, and it comes after three previous revolutions that Floridi associates with Nicolaus Copernicus, Charles Darwin, and Sigmund Freud respectively.

The essence of the fourth revolution is the realisation that humans are intrinsically informational, that we are ‘above all information processors, and our capacities in this regard are not uniquely biological.’ As such, the fourth revolution is occurring as a result of the development of computer science and ICTs. However, its impact is not simply technological; instead it is affecting the human conception of the world and their place within it. According to Floridi, ICTs

have not only provided unprecedented epistemic and engineering powers over natural and artificial realities; but by doing so they have also cast new light on who we are, how we are related to the world, and hence how we understand ourselves. Today, we are slowly accepting the idea that we are not Newtonian, standalone, and unique entities, but rather informationally embodied organisms (inforgs), mutually connected and embedded in an informational environment, the infosphere.

Floridi describes the way in which ICTs are transforming the world as a process of ‘reontologisation’. This notion refers to the radical re-engineering or re-design of something (any system, for example a machine or artefact) to a degree that ‘fundamentally transforms its

---

37 As the chair of the group of scholars however, it is likely that he contributed to the shape of those arguments. See Floridi (2015b), pp 1-3.
40 In essence, Floridi maintains that:
   today we acknowledge that we are not immobile, at the centre of the universe (Copernican revolution), we are not unnaturally separate and diverse from the rest of the animal kingdom (Darwinian revolution), and we are very far from being standalone Cartesian minds entirely transparent to ourselves (Freudian or neuroscientific revolution).
41 Demir (2010), p 3.
42 Byron (2010), p 136. According to Wolfgang Hofkirchner, the essence of Floridi’s overarching argument is that: the fourth revolution associated with ICTs imposes an unescapable infosphere on humans in which they are transformed into informational agents; this increases the importance of the management of the information life cycle; and this in turn requires ethical considerations that shape the infosphere. Hofkirchner (2010), p 178. For Hofkirchner’s reconstruction of this argument in light of his own criticisms, see Hofkirchner (2010), p 180.
intrinsic nature, that is, its ontology or essence."44 The term ‘infosphere’ in turn is based on the notion of ‘biosphere’, and is used to describe not only the natural environment or digital environments like cyberspace, but also the entire informational environment constituted by information entities.45 It refers to:

the whole informational environment constituted by all informational entities, their properties, interactions, processes, and mutual relations. It is an environment comparable to, but different from, cyberspace, which is only one of its sub-regions, as it were, since the infosphere also includes offline and analogue spaces of information.46

In the context of Floridi’s philosophy of information and the idea that everything can be viewed in informational terms, the infosphere is thus the entire environment constituted by information entities.47

ICTs are therefore reontologising the world transforming it into an infosphere. The main ways in which this is occurring is through the shift from analogue to digital and the growth in informational spaces.48 Digital tools and digital resources are converging to the point that ‘there is no ontological difference between processors and processed’.49 As such, ICTs are changing the fundamental nature of even everyday objects, from fridges to cars, which are increasingly becoming capable of processing information and capable of interaction.50 Hence they are being transformed into information entities and they operate in a growing information space. In addition to reontologising existing objects that are becoming seamlessly embedded into the everyday, ICTs are also creating new realities and blurring the distinctions between being online and offline – ‘the digital-online is spilling over into the analogue-offline and merging with it’.51 This is coupled with the increasing virtualisation of

---

46 Floridi (2014), p 41. See also Floridi (2013), p 6; Floridi (1999), p 44. Floridi argues that as an evolving concept, the infosphere ‘can also be used as synonymous with reality, once with interpret the latter informationally.’ See Floridi (2014), p 41. Elsewhere, Floridi writes that ‘it is a concept that, given an informational ontology, can also be used as synonymous with reality’, see Floridi (2013), p 6.
47 According to Hongladarom it is ‘the whole environment in which information plays a key, constitutive role; that is, the sum total of all information there is in a given environment.’ Hongladarom (2008), p 176. On how this concept has been used in relation to computer game environments for example, see Sicart (2011).
49 Floridi (2013), p 7 (emphasis in original).
services and resources\textsuperscript{52} to the point at which, according to Floridi, the human perspective on the ultimate nature of reality is changing from a materialist one into an informational one.\textsuperscript{53} Therefore, ICTs are changing the nature of everyday objects and processes, and creating new realities within which those objects and even humans, from an informational perspective, interact and exist in. This results in the transformation of the world into an infosphere – a world in which, when understood informationally, everything from natural environments to artificial virtual environments, and from humans to computer software, coexist and interact.

\textit{1.3 The Impact of ICTs and the turn to Information Ethics}

As a result of these transformations and the impact of ICTs, Floridi argues that new conceptual toolkits are required to make sense of the challenges that are brought about by technology in this context. Others have noted this too, namely that the development of computer technologies and the new forms of behaviour that they have made possible (or the substantial changes in the scope and scale of actions that are now possible) has raised new issues requiring novel theoretical approaches.\textsuperscript{54} Accordingly, Floridi argues that there is a need to consider the conceptual nature and implications of these developments\textsuperscript{55} in order to ensure a better understanding of ‘its nature, its less visible implications, and its impact on human and environmental welfare’.\textsuperscript{56} Therefore, according to Floridi there is a need to rethink the philosophical foundations on which existing concepts are based. Floridi’s philosophy of information aims to contribute to this and it provides the basis for his information ethics.

As such, in light of the recurring concern about the relationship between the natural and the technological, Floridi’s framework is based on a view of the world as an infosphere.

\textsuperscript{52} Floridi (2013), p 12.
\textsuperscript{53} Floridi writes that ‘[w]e are changing our everyday perspective on the ultimate nature of reality from a historical and materialist one, in which physical objects and mechanical processes play a key role, to a hyperhistorical and informational one.’ Floridi (2014), p 50.
\textsuperscript{55} Floridi writes that:

The development of information and communication technologies (ICTs) has not only brought enormous benefits and opportunities but also greatly outpaced our understanding of their conceptual nature and implications, while raising problems whose complexity and global dimensions are rapidly expanding, evolving, and becoming increasingly serious.

Floridi (2009), p 154.
\textsuperscript{56} Floridi (2009), p 154.
in which natural and technological environments are intertwined. One commentator has noted how from this perspective the relationship between humans and technology is ‘intrinsically interrelated.’ Floridi’s view stands in contrast to the modern view of technology which sees reality as the natural environment that is capable of being mastered and controlled by humanity. He argues that, besides the natural environment, humans also need to be concerned with the non-natural environments that they have created and which are increasingly intertwined into the natural environment. He maintains that:

In less than a century, we have moved from a state of submission to nature, through a state of power of potential total destruction, to the present state in which we have the means and tools to engineer entire new realities, tailor them to our needs and invent the future. For the first time in history, we are responsible for the very existence of whole aspects of our new environment.

Hence revitalising also the tensions between the ancient Greek notions of physis and technē, Floridi maintains that a practical reconciliation of the two is required, as ‘[i]nformation societies increasingly depend upon technology to thrive, but they equally need a healthy, natural environment to flourish.’ Accordingly, he suggests that the best way to think about the novel ethical problems is as environmental ones, and hence a new environmental ethics is needed for the information society. In this context, and as a branch of his philosophy of information, Floridi’s information ethics provides a framework that is concerned with the ethical impact of ICTs on human life and society.

Section 2: Information Ethics

The aim of information ethics is to guide the behaviour of a responsible and caring agent in the infosphere – the world pervaded by information entities and organisms that in various ways store, process and interact with information. It provides what can be described as an environmental ethics of the information age – a form of synthetic environmentalism that

58 Floridi (2001), p 63.
60 Floridi (2013), p 305.
61 Floridi (2001), p 66. Hongladarom maintains that Floridi’s view is ‘an adaptation of the ancient view’ on ethics in which nature, in the form of the infosphere, is given supreme importance. See Hongladarom (2008), p 182.
62 Floridi (2013), p xii. For an overview on the evolution of Floridi’s information ethics as a project, see Capurro (2008), pp 167-168.
63 Floridi maintains that:
takes the approach of deep ecology even further. Others have noted that it offers a ‘new ontological perspective’ from which to address the moral concerns particularly raised by, but not limited to, ICTs. Instead of an approach tailored towards specific technologies, it focuses on the more fundamental informational nature that all technology (and everything else) shares. It seeks to provide a more impartial and universal approach to ethics than traditional ethical theories, and promises a form of universal applicability in a world of moral pluralism. Therefore, information ethics has the promise of providing a novel normative framework particularly suited to addressing ethical concerns raised by the use of ICTs. Despite its promises, it has been subject to a range of criticisms. As will be demonstrated, especially information ethics’ principle of ontological equality, whereby all entities are afforded a basic right to exist and flourish, and the notion of entropy as evil, have been questioned. Before discussing these criticisms however, this section will first describe the key concepts and principles of information ethics.

2.1 Information Entities and the Infosphere

Information ethics is concerned not simply with the wellbeing of the natural environment or the biosphere, but with that of the infosphere. The infosphere is the totality of all entities that can logically exist, when they are understood informationally. Therefore, human beings, technological artefacts and everything else can be understood in informational terms and considered as information entities. Accordingly, the ethical discourse of information ethics:

---

one of the most fruitful contributions for developing an environmental approach comes from pre- or non-industrial cultures, which have been able to maintain a non-materialistic and nonconsumistic approach to the world. These cultures are still spiritual enough to perceive in both physical and immaterial realities something intrinsically worthy of respect, simply as forms of existence.


Synthetic here refers to the use of the term both in the holistic/inclusive and artificial sense. See Floridi (2013), p 18.

Deep ecology, rejecting the anthropocentric view of nature as only having instrumental value to humans, holds that it has intrinsic value in itself, see Dusek (2006), p 187. See also Naess (1973).

Brenner (2010), p 111.

Durante (2010b), p 151.

According to Hongladarom, it does so by grounding itself in the idea that ‘underlying reality which is presupposed and shared by all parties whose viewpoints are diverse.’ Hongladarom (2008), p 175. Further, he notes that instead of the value of the individual that underpins liberal theories, for Floridi instead it is ‘the whole ontic substance, the whole of reality itself’ undergirding the value. Hongladarom (2008), p 184.


Floridi (1999), p 44.
concerns any entity, understood informationally, that is, not only all persons, their cultivation, wellbeing, and social interactions, not only animals, plants, and their proper natural life, but also anything that exists, from paintings and books to stars and stones; anything that may or will exist, like future generations; and anything that was but is no more, like our ancestors or old civilizations.\(^{71}\)

The way in which information ethics considers all entities as information entities is by perceiving the world from an informational perspective.\(^{72}\) As mentioned, key to this is conceptualising information as data structures, ‘equivalent to patterns or entities in the world.’\(^{73}\) This is in contrast to purely viewing information semantically, as the contents of an encyclopaedia for instance, though naturally this is also included within the former conceptualisation.\(^{74}\) The purpose of this informational perspective, or its ‘level of abstraction’ in Floridi’s terminology, is a grounding of information ethics to the lowest common denominator shared by everything, namely information.\(^{75}\) As such, viewing things informationally means that everything can be abstracted to a sufficient degree and viewed as information entities. Consider for instance a human being and the various levels of abstraction or ways in which they can be perceived: as ‘a primate, a mammal, a vertebrate, a colony of eukaryotic cells, and a congeries of subatomic particles’.\(^{76}\) The highest and most inclusive level of abstraction however, is informational.\(^{77}\) Therefore, all entities are regarded in similar terms as information entities. By adopting this perspective, information ethics

---

\(^{71}\) Floridi (2010a), p 113.

\(^{72}\) The level of abstraction is in some ways the point of view from which to analyse things – the perspective and degree of abstraction from which things are conceptualised. Specifically, it is defined as ‘a finite but non-empty set of observables, which are expected to be the building blocks in a theory characterised by their very choice.’ Floridi (2013), p 32. Information ethics is ‘committed to a LoA [level of abstraction] that interprets reality—that is, any system—informationally.’ Floridi (2013), p 35.

\(^{73}\) Floridi (2010a), p 110. For a critique of Floridi’s conception of information, see Adriaans (2010). See also Floridi’s reply, Floridi (2010b), pp 259-260.

\(^{74}\) Floridi maintains that all entities will be described as clusters of data, that is, as informational objects. More precisely, our agent A (like any other entity) will be a discrete, self-contained, encapsulated package containing (i) the appropriate data structures, which constitute the nature of the entity in question, that is, the state of the object, its unique identity, and its attributes; and (ii) a collection of operations, functions, or procedures, which are activated by various interactions or stimuli (that is, messages received from other objects or changes within itself), and correspondingly define how the object behaves or reacts to them. At this level of analysis, informational systems as such, rather than just living systems in general, are raised to the role of agents and patients of any action, with environmental processes, changes, and interactions equally described informationally.

Floridi (2010a), p 111.

\(^{75}\) Brenner (2010), p 111.

\(^{76}\) Doyle (2010), p 164.

\(^{77}\) Doyle (2010), p 164.
expressly commits itself to an informational ontology ‘whereby human beings as well as animals, plants, artefacts and so forth are interpreted as informational entities.’

In doing so, it seeks to provide a universal and impartial (or at least less biased) ethics. Hence it aspires to be an all-inclusive ethics. First, the environment with which it is concerned is not simply the biophysical environment as ‘the infosphere includes also any other environment.’ Hence the natural environment, and the Internet and other digital environments that make up cyberspace, are all considered as part of the infosphere. Second, all entities – be they books, robots or humans – are considered as information entities and as part of the infosphere. Accordingly, information ethics seeks a higher degree of impartiality and universality, by expanding the concept of what counts as the centre for moral claims to include ‘every instance of information, no matter whether physically implemented or not.’

For Floridi this is the logical expansion of what counts as having moral value, to the all-inclusive position in which no line is drawn at all and everything is included within the moral circle. However, while all entities are considered to have moral value, ‘they do not share the same degree of dignity.’ Information ethics ‘does not treat human beings as if they were no more important than animals or trees or indeed stones.’ It is important to note that the minimalism it advocates is only methodological: it simply holds ‘the view that entities can be analysed by focusing on their lowest common denominator, represented by an informational ontology.’ Information ethics assigns worth to all entities in their capacity as information.

Therefore, information ethics attaches a basic degree of value to all entities that collectively form the infosphere. It advocates that ‘[n]ot only inanimate but also ideal, intangible or intellectual

---

78 Floridi (2006), p 33. Floridi uses the terms information(al) entities and information(al) objects interchangeably.
80 Floridi (1999), p 50.
81 As Joseph Brenner notes, in Floridi’s information ethics, ‘[i]nformational systems as such, rather than just living systems in general, are raised to the role of agents and patients of any action, with environmental processes, changes, and interactions are equally described informationally.’ Brenner (2010), p 124.
82 Floridi (1999), p 43. Elsewhere, Floridi writes that information ethics is ‘impartial and universal because it brings to ultimate completion the process of enlargement of the concept of what may count as a centre of a (no matter how minimal) moral claim, which now includes every instance of being understood informationally … no matter whether physically implemented or not.’ Floridi (2006), p 26.
83 Doyle (2010), pp 164-166. Tony Doyle however is critical of this. He maintains that merely highlighting ‘an apparent trend in moral philosophy towards greater inclusiveness’, whatever its merits, ‘is not an argument for expanding the moral circle.’ Doyle (2010), p 166 (emphasis in original). For Floridi’s reply, see Floridi (2010b), pp 269-273.
84 Floridi (1999), p 50.
objects can have a minimal degree of moral value, no matter how humble, and so be entitled to some respect. In doing so, it seeks to provide a more inclusive, universal and impartial ethics concerned with all environments and entities.

2.2 The Ontological Equality Principle

Consequently, from this perspective, everything in the world can be conceptualised as information entities and as part of the infosphere. Central to the ethical framework of information ethics is the principle of ontological equality which essentially refers to the idea that everything should have a basic right to exist. According to Floridi, every information entity ‘simply for the fact of being what it is, enjoys an initial, overridable, equal right to exist and develop in a way which is appropriate to its nature.’ As such, every entity has some intrinsic moral value (however minimal and overridable) and is entitled to ‘some equally minimal degree of moral respect’. This basic right of every entity to exist is fundamental:

...every entity, as an expression of being, has a dignity, constituted by its mode of existence and essence (the collection of all the elementary properties that constitute it for what it is), which deserve to be respected and hence place moral claims on the interacting agent and ought to contribute to the constraint and guidance of his ethical decisions and behaviour.

Accordingly, pursuant to the ontological equality principle, all information entities should be morally respected as part of the infosphere to which they belong. Through this principle, information ethics seeks to adopt a more encompassing approach to viewing the world, one that is not even biased against the ‘inanimate, lifeless, intangible, or abstract’.

---

89 Floridi (1999), p 44. Elsewhere, Floridi writes that information ethics holds that every entity, as an expression of being, has a dignity, constituted by its mode of existence and essence (the collection of all the elementary properties that constitute it for what it is), which deserve to be respected (at least in a minimal and overridable sense) and hence place moral claims on the interacting agent and ought to contribute to the constraint and guidance of his ethical decisions and behaviour. Floridi (2006), p 26. This notion, according to Doyle, is comparable to ‘the utilitarian principle that everyone’s happiness (or interests or preferences) be weighed equally or to [John] Rawls’s assumption that the veil of ignorance ensures equality for the contractors in the original position.’ Doyle (2010), p 165. See also Hongladarom (2008), p 184.
90 Floridi (2006), p 30. Floridi maintains that information ethics is premised on the argument ‘that entities deserve respect because they have intrinsic value, not that if entities deserve respect then they have intrinsic value.’ Floridi (2008b), p 192 (emphasis in original).
91 Floridi (1999), p 44.
92 Durante (2010b), p 150.
93 Floridi and Sanders (2004a), p 92.
entities, and not simply human beings for example, are understood as enjoying some basic right to exist. Tied to every entity’s right to exist is the right to flourish – ‘to improve and enrich its existence and essence.’

2.3 Goodness/Being and Evil/Entropy

Information ethics thus regards the right of an entity to exist and flourish as fundamental. Being (as opposed to ‘life’) and every entity’s contribution to the wellbeing of the infosphere make up the basic notions of what is good. In contrast, evil is considered in terms of entropy (as opposed to ‘suffering’). In this context, the notions of being and goodness are intertwined and intrinsic to all entities simply by virtue of their existence. Hence every entity’s right to exist should be considered in the context of the entire infosphere that it forms part of, and avoiding negative effects (entropy) therein. As such, information ethics seeks to evaluate the moral duty of any

being in terms of [its] contribution to the growth of the infosphere, and any process, action or event that negatively affects the whole infosphere – not just an information entity – as an increase in its level of entropy and hence an instance of evil.

Information ethics therefore sees the world as made up of information and as fundamentally good, and any acts that damage it as evil. As such, opposed to focusing its concern with the actions, characters or values of a human actor, information ethics shifts its focus towards considering the evil suffered by information entities and the infosphere.

As mentioned in chapter 1, Floridi adopts a very particular definition of the notion of entropy. In information ethics, entropy is defined as referring to ‘any form of impoverishment of Being’ – that is, ‘any kind of destruction or corruption of entities understood as informational objects’.

Here destruction refers to ‘the complete annihilation of the entity in

---

94 Floridi (1999), p 45.
95 Durante (2010b), p 152. See also Floridi (2008b), p 201; Floridi (2013), pp 322-323. For a pluralistic conception of being from an informational viewpoint, see Durante (2010b), p 158.
96 Floridi (1999), p 45. Elsewhere, Floridi writes that: ‘information ethics evaluates the moral duty of any information agent in terms of contribution to the growth of the infosphere and any process, action, or event that negatively affects the whole infosphere – not just an informational entity – as an increase in its level of entropy and hence an instance of evil.’ Floridi (2010a), pp 112-113 (emphasis in original).
98 Floridi (2013), p 67 (emphasis in original). Elsewhere, Floridi writes that it ‘refers to any kind of destruction, corruption, pollution, and depletion of informational objects (mind, not just of information as semantic content),
question’, for instance where it is entirely erased and completely ceases to exist.  

Corruption in turn refers to ‘a form of pollution or depletion of the entity’ that is comparable to its degradation.  

As such, entropy (evil) is understood in a metaphysical sense as the destruction or corruption of any entity that enjoys an inherent right to exist, that is, the destruction or corruption of its being (goodness).  

The term is therefore used differently than, for example, in thermodynamics or in Shannon’s information theory.  

In light of these concepts, information ethics provides four moral laws to guide behaviour within the infosphere. These are:  

0. entropy ought not to be caused in the infosphere (null law)  
1. entropy ought to be prevented in the infosphere  
2. entropy ought to be removed from the infosphere  
3. the flourishing of informational entities as well as of the whole infosphere ought to be promoted by preserving, cultivating and enriching their wellbeing.  

These principles are designed to provide guidance on the actions of a responsible and caring agent within the infosphere. They are ranked in order of moral value, thus acting contrary to that, any form of impoverishment of reality.’ Floridi (2010a), p 112 (emphasis in original). Thus he argues that:  

By defending the intrinsic moral worth of informational objects, IE [information ethics] does not refer to the moral value of an email, of the Britannica, of Newton’s Principia, or of any other piece of well-formed and meaningful data. What IE suggests is that we adopt an informational LoA [level of abstraction] to approach the analysis of being in terms of a minimal common ontology, whereby human beings as well as animals, plants, artefacts and so forth are interpreted as informational entities. IE is not an ethics of the BBC news. Floridi (2006), p 33 (emphasis in original).  

100 Floridi (2013), p 67.  
102 See Floridi (2013), pp 65-67. Floridi writes that:  

Both in thermodynamics and in information theory, entropy is a syntactic and quantitative concept: neither information nor entropy refers to the actual meaning, content, interpretation (semantics), or to the existence and nature (ontology) of the system. In IE, we still treat the two concepts of information and entropy as being related, but we are concerned with the semantic and ontological nature of information. For example, as the infosphere becomes increasingly meaningful and rich in content, the amount of information increases (what one may call, for the sake of clarity) metaphysical entropy decreases. Thus, in IE, entropy is not merely a syntactic concept, but, as the opposite of semantic and ontic information, it indicates the decrease or decay of information leading to absence of form, pattern, differentiation, or content in the infosphere. It is therefore most emphatically not the physicists’ or engineers’ concept of entropy. Floridi (2013), pp 66-67 (emphasis in original).  

103 Floridi (2013), p 47.  
the null law is morally worse than the third principle for example. The general approach is to consider whether the overall state of the infosphere is better, even if some entropy is caused, hence the concern is with the global levels of entropy opposed to minor fluctuations.\textsuperscript{105} It is important to note that the destruction or other form of impoverishment of the infosphere is not merely about the destruction of information, but about the destruction of information entities in their capacity as such.\textsuperscript{106} Therefore, from this perspective, harm or damage to an entity is considered in terms of the degradation of its being that is evident, for instance, in the corruption of its properties or in its complete destruction and the consequent increased levels of entropy in the infosphere.

With these principles Floridi seeks to provide an ethical framework that affords ‘respect for both the physical and the immaterial world.’\textsuperscript{107} He maintains that an environmental approach that focuses on the wellbeing of the infosphere is best suited for this. He writes that:

Reality, both natural and immaterial, is not merely available for domination, control, and exploitation. Reality should also be an object of respect in its autonomous existence. This is what we can learn from an environmental approach.\textsuperscript{108}

Therefore, in summary, Floridi’s information ethics is an environmental ethics that is concerned with the wellbeing of the infosphere. The infosphere is the totality of everything that exists – it is constituted by everything, from humans, to rocks, to computer viruses, and natural and virtual environments. The infosphere can be conceptualised as synonymous to reality itself once an informational level of abstraction is adopted. The level of abstraction is crucial to information ethics, and it expressly adopts an informational one. This means that all objects in the world are perceived in informational terms – that is, on a relatively high level of abstraction – and seen as information entities. In doing so, it does not seek to raise animals or objects to the level of humans, nor lower humans to the level of objects. Instead, for methodological purposes, it simply perceives everything from an inclusive (informational) perspective so that they share a common denominator. This also places emphasis on the foundational nature of information (everything can be described as such) and its importance

\textsuperscript{105} See Floridi (2013), pp 71-72.
\textsuperscript{106} Durante (2010b), p 157.
\textsuperscript{107} Floridi (2001), p 67.
\textsuperscript{108} Floridi (2001), p 67. Hongladarom maintains that these principles form a clear basis for an environmental ethics, a motto of which could be ‘let all things flourish.’ Hongladarom (2008), p 176.
in information societies increasingly dependent on ICTs that process information. As a result, given its informational ontology and concern with the overall wellbeing of the infosphere, information ethics provides a unique way of seeing the world pervaded by ICTs. It takes the position that all entities have a basic right to exist and flourish. Being or existence is regarded as good and taken to be more fundamental or basic than simply ‘life’. In contrast, evil is understood in terms of entropy: the destruction or corruption of information entities. A responsible agent in this context seeks to avoid increasing the levels of entropy in the infosphere and strives to promote the right of all other information entities to flourish.

2.4 Criticisms

Information ethics has been subject to a range of criticisms which highlight and question the radical nature of some of its claims. For example, criticisms have been levelled against the ontological equality principle and the reasons for why all entities should be provided moral respect. Also subject to criticism has been the perceived reduction of everything from humans to inanimate objects into information entities, and information ethics’ consequent inability to assess the differences in value that should be afforded to these entities. Finally, the viability of the notion of entropy as evil, that is, where an information entity is damaged or destroyed violating its natural right to exist and flourish, has been criticised. These particular criticisms will be the focus here as they aid in the explanation of information ethics’ conceptual foundation. What follows is first an account of these criticisms and then Floridi’s responses to them.

2.4.1 The ontological equality principle and value conflicts

Many have questioned the ontological equality principle and the reasoning behind why all information entities should have moral value. Michael Byron for example is critical of Floridi’s all-inclusive broadening of the moral scope of information ethics. He maintains that because information is ontologically basic – as everything is constituted by information – it is odd to attribute intrinsic value to mere being in this sense. This leads to the position that since information itself is valuable, it requires people to seek maximal quantities of

---

109 For a convenient collation of these and other criticisms that have been made against information ethics, and Floridi’s reply to those criticisms, see Floridi (2013), chapter 16.
110 Byron (2010), p 142. See also Floridi’s reply, Floridi (2010b), pp 267-269.
information to make the universe a morally better place.\footnote{111} Similarly, Philip Brey argues that information ethics does not provide a sound justification for its foundational claim that everything deserves some moral respect for its existence as an information object.\footnote{112} He argues that often there are other reasons for which objects are valued.\footnote{113} Tony Doyle also questions for example what it means for a waterfall to flourish and why this in itself should be valued. He suggests that it would be more reasonable to attach value to natural wonders and animals for example, where humans attach value to them or their conservation.\footnote{114} Doyle argues that Floridi only provides an ‘undefended claim that all information objects have an essential moral dignity.’\footnote{115} Others have echoed these concerns, arguing that there tend to be other reasons to respect or value objects, besides their inherent ‘birthright’ as information objects.\footnote{116} Essentially these authors question why information entities as such should have moral value merely due to their existence, as the ontological equality principle asserts.

Another related criticism is that, if all entities can be considered as information entities that deserve a basic level of moral respect pursuant to the notion of ontological equality, then how can or should an assessment be made about when one entity should be respected more than another? This has been raised by some authors who argue that information ethics does not provide a sufficient framework to assess this. Byron for example argues that Floridi provides no means of assessing which information entity is more valuable, for instance when comparing a human and a rock.\footnote{117} Brey also makes this criticism, noting that information ethics fails to give the means to distinguish between the value of a human being and toxic waste for instance.\footnote{118} Similarly, Bernd Stahl points out that Floridi does not provide a means of addressing value conflicts between entities.\footnote{119} Soraj Hongladarom also highlights this on a wider level, arguing that information ethics does not provide the means to

\begin{itemize}
  \item Byron (2010), p 142. See also Floridi’s reply, Floridi (2010b), pp 267-269.
  \item Brey (2008), p 111.
  \item Doyle (2010), pp 166-167.
  \item Doyle (2010), p 168. For Floridi’s reply, see Floridi (2010b), pp 269-273.
  \item Volkman (2010), p 395. Volkman maintains that what a thing is, and whether and how it should be respected depends on the purposes and values that are attached to it by people – something the principle of ontological equality and information ethics’ universalism and impartialism do not capture. Volkman (2010), pp 393-394. For Floridi’s reply, see Floridi (2010c), pp 414-417. Similarly, Rafael Capurro maintains that value is generally a relationship and not merely a property of an object. See Capurro (2008), p 168. See also Floridi’s reply, Floridi (2008b), pp 199-201.
  \item Byron (2010), p 142. See also Floridi’s reply, Floridi (2010b), pp 267-269.
  \item Stahl (2008), pp 103-104. See also Floridi’s reply, Floridi (2008b), pp 190-191.
\end{itemize}
prioritise different value systems.\textsuperscript{120} Therefore, based on the principle of ontological equality pursuant to which all entities are equal on a basic level, according to these authors information ethics fails to provide practical guidance on how to prioritise or assess the differences in value between information entities.

2.4.2 Entropy as evil

In addition to these criticisms against the ontological equality principle and the assessment of value conflicts, many also question what it means for an information entity to flourish and whether, as according to the four principles provided by Floridi, all forms of entropy are morally evil. For example, Byron argues that the destruction of any object is unethical following these principles:

Cyclones, volcanic eruptions, and tornadoes all cause moral evil when they destroy things—people, artifacts, or natural objects. When a star explodes, that’s a deeply unethical event, given the extent of destruction.\textsuperscript{121}

Besides these natural events, Mikko Siponen has questioned whether human activities, such as fishing, hunting or felling trees, would be considered morally wrong using these principles because in each instance information entities are stripped of their rights to exist.\textsuperscript{122} Further, there has even been criticism about the operation of information ethics in the context of ICT specific issues such as computer viruses and the use of anti-virus software. For instance, Rafael Capurro maintains that these principles contradict the deletion of viruses, unsolicited emails, and other forms of less useful information.\textsuperscript{123} Siponen also considers computer viruses in this context: from an information ethics perspective a virus would be regarded as an information entity as it is made up of a packet of information. As viruses are designed to spread and destroy information, meaning these functions are key to their nature and flourishing, then anti-virus activities in themselves would be morally wrong.\textsuperscript{124} Accordingly, these authors are critical of what it means for an entity to flourish and whether any instance of entropy that diminishes an entity’s natural right to flourish can be regarded as morally evil.

\textsuperscript{120} Hongladarom notes the difficulty of how to prioritise different value systems (for example, North American and European Union models of privacy) from an information ethics approach. See Hongladarom (2008), p 186.
\textsuperscript{121} Byron (2010), p 144. See also Floridi’s reply, Floridi (2010b), pp 267-269.
\textsuperscript{122} Siponen (2004), p 287.
\textsuperscript{123} Capurro (2008), p 170. See also Floridi’s reply, Floridi (2008b), pp 199-201.
\textsuperscript{124} Siponen (2004), p 287.
2.4.3 Floridi’s responses

In defence of information ethics, Floridi has responded to these criticisms. In relation to the criticism levelled against the ontological equality principle and the reasoning behind why all information entities should be given moral respect, he maintains that information ethics is not simply about expanding the scope of ethical discourse from human and biological agents to artificial, digital, or informational realities. Instead, it is about completely changing the perspective to an informational one, through which all entities are interpreted informationally, and this in turn means that everything including human, animal, social and artificial entities are included. From this informational level of abstraction, human beings are not simply reduced to information entities equal to rocks or toxic waste – Floridi emphasises the point that the informational ontology is simply the lowest common denominator of everything. It is not meant to reduce humans to numbers but instead, he argues that, like the Darwinian account of humans as part of the animal kingdom that enabled humans to see themselves differently, if humans can be perceived as information organisms with reality understood as an infosphere, then it makes sense to adopt an informational ontology. Therefore, the reason why, besides humans, all other entities should be respected and considered as having intrinsic worth, is that this should be considered the starting point. Floridi argues that:

because we have no reasons against the intrinsic value of Being in all its manifestations, we should expand an environmental approach to all entities, including non-sentient beings. The injunction is to treat something as intrinsically valuable and hence worthy of moral respect by default, until ‘proven guilty’.

Thus he argues that all things should be respected because they have intrinsic value, and not that if they have intrinsic value then they should be respected. Accordingly, the ontological equality principle is based on the idea that everything, in its capacity as an information entity, should be afforded a basic level moral respect as a starting point. This does not mean however, that all entities are equally valuable in their contribution to the wellbeing of the entire infosphere.

Following from this generally, and in relation to the assessment of the intrinsic value of different information entities specifically, Floridi maintains information ethics is not simply about comparing the value of two information entities. He argues that it is ultimately not about comparing the intrinsic value of, for example, a work of Shakespeare with an ‘airport novel’. Instead, he maintains that the issue is whether ‘Goodness and Being … might be two sides of the same concept, as Evil and non-Being might be.’ Like many Eastern and Western philosophical traditions, he adopts this line of reasoning, arguing that there is a need to update the human conception of the universe ‘in terms of an informational ontology, whereby Being is understood informationally and non-Being in terms of metaphysical entropy.’

In more practical terms, the assessment of whether one entity has more value than another entity is ultimately qualitative involving a consideration of its contribution to the overall wellbeing of the infosphere: the higher it is, ‘the higher its status is in the chain of morally respectable things.’ For instance, a biological virus must ‘be destroyed for the sake of the rest of the environment and its flourishing.’ As such, the moral laws of information ethics are intended as basic principles that can assist in making these value assessments. Just like in environmental ethics, Floridi argues that simply ‘[h]aving some universal, basic, and robust principles in place helps enormously when it comes to dealing with particular, complex, practical matters.’

Collectively, the criticisms against information ethics that have been highlighted here essentially question the appropriateness of the notion of ontological equality and whether any form of entropy should be regarded as evil. They question the idea that not just humans or living organisms but all entities should be afforded moral respect; and whether the destruction or corruption of these entities is morally evil and should be avoided on that basis. Indeed, a degree of acceptance is needed of the wider arguments that Floridi makes about the profound impact of ICTs, the informational nature of reality, and the resulting appropriateness of an environmental approach based on information. However, particularly due to its radical nature, information ethics provides a unique approach, grounded in a philosophy of information, and promises a conceptual framework through which to consider the ethical issues surrounding ICTs. It provides a framework through which to understand the

---

130 Floridi (2013), pp 322-323.
world in informational terms and enables a rethinking of what it means for an entity to be harmed – even a non-human or non-material entity such as an information process – within the wider context of the transformations brought about by the development of ICTs. As such, it offers the conceptual basis on which the increasing importance of information (be it in the everyday life of human beings or in relation to the functioning of modern states as information societies) can be taken seriously. Drawing on this framework, the subsequent chapters will demonstrate how the law’s existing conceptual foundations remain grounded in anthropocentrism and materialism, and how an informational approach offers a means through which to rethink these foundations in informational terms.

Conclusion

This chapter described Floridi’s information ethics in order to lay the conceptual foundations on which this thesis will develop an informational approach. The first section located information ethics within Floridi’s philosophy of technology more generally. The second section defined the principles and concepts of information ethics, including the notion of ontological equality, the infosphere, and entropy. It also considered the criticisms that information ethics has faced. Collectively, it was demonstrated that information ethics provides a novel form of environmental ethics for the information age.
Chapter 3: Technology, Violence, and Law

Introduction

This chapter argues that an informational approach offers a means to reconceptualise the state as an information entity and the notion of violence in terms of entropy. Doing so enables international law to recognise the forms of ‘informational violence’ that cyber attacks can cause. This chapter consists of four sections. The first section briefly considers the prevalence of global information flows that have historically called for international legal responses. It also outlines how the international community has recognised the increasing importance of ICTs to the functioning and prosperity of modern societies. The second section explores international law and the containment of violence, that is, international law’s central concern to regulate warfare and limit physical violence. Section three then considers how cyber warfare challenges the traditional understanding of warfare, in what is identified as an ontological gap between kinetic and cyber warfare. Finally, drawing on information ethics, section four provides an informational reconceptualisation of the state and the notion of violence. It is argued that an informational approach offers a means to broaden international law’s containment of violence to also forms of informational violence, and it enables recognition of how cyber attacks can harm the state as an information entity.

Section 1: International Law and Information

Vast amounts of information or data flow across the globe – in 1992 the amount of Internet traffic was approximately 100 gigabytes per day, whereas in 2014, this figure was approximately 16,000 gigabytes per second.¹ Indeed, given various developments such as the increased globalisation of the global economy, increase in data transfer between public and private sectors, and vast increases in the volume of existing data and its transfer and processing; information itself has become a ‘crucial raw material’ in the global economy.² Since the early development of ICTs and the ability for information to be transferred across the world – between governmental, corporate, and individual actors, and done so instantaneously with little regard for territorial borders – there have been calls to regulate

---

these data flows. The concerns for the regulation of these data flows date back to the 1970s and 1980s, when there was already a sense that information, in the context of ‘transborder data flows’, was becoming increasingly important.³ The development and fusion of computer and telecommunication technology was seen to lead to the growth of information societies, that is, societies in which ‘information is a predominant factor in economic, social, political and other important facets of life.’⁴ Already then, information was regarded as the successor to industrial processes, similar to the way in which mechanical systems were succeeded by electronics.⁵ A range of concerns were associated with these developments, centred primarily at the time on economic development and the protection of personal privacy. For instance, in 1980 the Organisation for Economic Co-operation and Development (OECD) issued guidelines for transborder data flows that sought to protect personal data while ensuring minimal barriers to these data flows given their economic advantages.⁶ Similarly, in a United Nations Educational, Scientific and Cultural Organisation (UNESCO) affiliated conference in 1984, the importance of regulating transborder data flows was highlighted. There was a call for instance to ‘create some kind of international highway code for informatics’ to regulate transborder data flows and avoid chaos, especially given that the technologies enabling these flows formed ‘the nervous system of nations’.⁷ It was also predicted that:

The next five to ten years will be crucial regarding the flow of data from one country to another: we can foresee that in the future it will not be territorial disputes or concerns of national supremacy but the control and possession of information that will be the source of major conflicts as this lies at the root of everything: of development, of security, of defence, of education, and of culture itself.⁸

³ According to Peter Robinson, the range of issues raised by increasing transborder data flows ‘are often complex and sensitive and are concerned with national sovereignty, national security, trade, competitiveness, productivity, regulation, employment, culture, and computer-related crime as well as privacy protection.’ Robinson (1987), p 369.
⁶ The group of government experts instructed to develop these guidelines was chaired by Michael Kirby. The aim of the guidelines was to ensure the harmonisation of privacy protection laws across the world and to ensure the free flow of data across the world, as restrictions on these flows were seen to cause serious disruptions to the economic sector. See Organisation of Economic Co-Operation and Development (1980) ‘Guidelines on the Protection of Privacy and Transborder Flows of Personal Data’, available at http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldatal.htm. See also Kirby (2010).
These predictions were made prior to the development of the World Wide Web, and the more recent ‘Internet of Things’ which describes the increasing ways in which ICTs are embedded into everyday objects enabling them to process and communicate information. However, these predictions demonstrate that already in the 1980s there was a sense that information was becoming more and more central, and rules were needed to regulate international data flows. Indeed, this need was foreseen to expand beyond merely the economic realm and that of personal privacy, and instead into all aspects of society and even into international security and conflict.9

In fact, even prior to these developments in the 1980s, early telegraphic communication technologies contributed greatly to an international concern to regulate new technologies that operated mostly regardless of national borders. The International Telegraph Union for example, as the first public international union, was formed as an international response to issues raised by new technology.10 It sought to promote the free flow of data by ensuring the telegraphic infrastructure of states was sufficient to ‘ensure the rapid transmission’ of information, and that this infrastructure could cater for state communications on a permanent basis, ‘day and night, without interruption.’11 In addition to promoting the free flow of data in this way, international law has also sought to limit the flows of information deemed harmful or contrary to international law. Information or data in this context refers to analogue data, that is, the transmission of telephone, telegraph, television, and radio data.12 For example, the 1936 International Convention concerning the Use of Broadcasting in the Cause of Peace13 sought to prohibit any transmission of information detrimental to or incompatible with the internal order of a state, that is, propaganda (Article

---

9 In 1980 a special issue of the *Stanford Journal of International Law* on transborder data flows was published, in which various authors highlighted the far reach of these issues involving everything from ‘personal privacy, political freedom, national economic development, cultural identity, and national sovereignty’ (Fishman (1980), p 1), and predicted that ‘political conflict about the direction, access, use, and control of transborder data flows can be expected.’ Novotny (1980), p 142.

10 According to Bob Reinalda, the nineteenth century international telegraph and postal unions ‘responded to the expansion of modern capitalism and technology, which did not take much notice of national borders’. Reinalda (2009), p 83.


12 Analogue communications, according to Henry Perritt, involve ‘representing real world intelligence, such as a sound wave, by an electric signal, with essentially the same characteristics of frequency and amplitude as the real world phenomenon.’ Perritt (1996), p 7. Digital communications in contrast, ‘take millions of samples of real world soundwave or video representation per minute and represent the sample features of the real world signal by arithmetic quantities, ultimately reduced to binary digits or “bits.”’ Perritt (1996), p 7.

1), and information that is false and consequently likely to harm ‘good international understanding’ (Article 3). Additionally, the International Telegraph Union’s successor, the International Telecommunication Union (ITU),\(^\text{14}\) has sought to allocate and register radio frequencies to ‘avoid harmful interference between radio stations of different countries’ and to ‘coordinate efforts to eliminate harmful interference between radio stations of different countries’.\(^\text{15}\) These provisions were also targeted at preventing offshore pirate radio stations in the 1950s and 1960s from broadcasting on unauthorised wavelengths and from broadcasting material that was being used without authorisation.\(^\text{16}\) They were aimed at controlling the flows of information that, for example, harmed the various political, social and economic interests of states. Similarly, Article 109 of the *United Nations Convention on the Law of the Sea* requires states to cooperate in the suppression of ‘unauthorised broadcasting’ from the high seas, thereby seeking to prevent ‘the transmission of sound radio or television broadcasts’ that are contrary to international law.\(^\text{17}\) Harmful interference to the radio services or communications of those authorised to broadcast them is also addressed by a later ITU convention,\(^\text{18}\) amounting to a general prohibition on deliberate radio interference or ‘jamming’.\(^\text{19}\) International law has therefore historically sought to regulate the international flow of information and deemed certain forms of information harmful.

Despite successful international efforts by states to regulate various analogue data flows, the current regulation and governance of digital data flows, for instance the Internet, stems from a more complex landscape of public and private actors.\(^\text{20}\) While originally regulated by a smaller technical community, the technical protocols and standards of the Internet are currently regulated by a combination of private actors such as the Internet

\(^{14}\) Established in 1865 as the International Telegraph Union, in 1932 it was transformed into the International Telecommunication Union, and in 1947 it became a specialised UN agency. See International Telecommunications Union, ‘History’, http://www.itu.int/en/about/Pages/history.aspx, accessed on 25 August 2015.


\(^{16}\) Hunnings (1965), pp 413-414.


\(^{19}\) De Brabantere (2012).

\(^{20}\) Lee Bygrave and Terje Michaelsen for instance, write that the governance of the Internet is rather wrought by a mélange of various bodies—private and public, old and new. Viewed from afar, the governance structure resulting from these bodies’ interaction appears relatively flat, open, sprawling, ad hoc, and amorphous. Lines of responsibility are blurred, as are lines of competence and funding. Many of the lines straddle if not eviscerate traditional organizational boundaries. Bygrave and Michaelsen (2009), p 92.
Corporation for Assigned Names and Numbers (ICANN) and increasingly the UN affiliated ITU, which itself is made up of states and non-state actors.\textsuperscript{21} When it comes to particular uses of the Internet, states have sought to restrict certain activities involving the use of computer systems and data. In addition to censorship laws and restrictions on harmful communications within states’ domestic jurisdictions,\textsuperscript{22} states have, for instance through international efforts such as the Convention on Cybercrime,\textsuperscript{23} deemed certain criminal uses of networks and improper use of information therein unlawful. For example, the Convention on Cybercrime seeks, through the harmonisation of national laws, to regulate certain harmful uses of networks and data. It includes illegal access to computer systems without right (Article 2), and the interception of non-public data being transferred between computer systems (Article 3). It also includes intentional interference, that is, the ‘damaging, deletion, deterioration, alteration or suppression of computer data’ (Article 4), and interference with the functioning of computer systems which refers to ‘the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering, or suppressing computer data’ (Article 5).\textsuperscript{24} Therefore, information in the context of the Internet and the harm that can stem from criminal activities in cyberspace are increasingly regulated by international law. However, the harmful data flows between states that have the potential to undermine international peace and security have only become a more recent concern, particularly given the increased dependence of states on digital ICTs.

Within the UN General Assembly, various resolutions on ‘Developments in the Field of Information and Telecommunications in the Context of International Security’ have been adopted yearly since originally introduced by Russia in 1998.\textsuperscript{25} Here the First Committee of the UN General Assembly (the Disarmament and International Security Committee) has highlighted a number of international issues surrounding the use of ICTs. These include the role of science and technology in relation to international security, and the positive

\textsuperscript{21} Despite its attempts however, the ITU has not been able to position itself as the primary regulator of the Internet like it has in telecommunications since the late nineteenth century. See Take (2012), p 506.
\textsuperscript{22} For instance, Chinese efforts to block, filter and monitor Internet traffic is often described as China’s ‘Great Firewall’, see Clarke and Knake (2010), p 57. New Zealand in 2015 passed a law protecting against harmful uses of digital communications, see Harmful Digital Communications Act 2015 (New Zealand).
\textsuperscript{25} The first resolution was adopted in 1999, see Developments in the Field of Information and Telecommunications in the Context of International Security (adopted by the UN General Assembly on 4 January 1999, UN Doc A/RES/53/70).
opportunities associated with these technologies in terms of developing civilisation, international cooperation, and the circulation of information. In addition to concerns that these technologies can be used for criminal or terrorist purposes, concerns have also been expressed that they ‘can potentially be used for purposes that are inconsistent with the objectives of maintaining international stability and security and may adversely affect the integrity of the infrastructure of States to the detriment of their security in both civil and military fields’. 26

The Second Committee (the Economic and Financial Committee) has in turn adopted a number of resolutions encouraging a ‘global culture of cybersecurity’. 27 These resolutions highlight a range of international issues relating to ICTs. The resolution adopted in 2003 for example notes the growing dependence of governments, businesses and other organisations, and individuals on information technologies; 28 and the threats and vulnerabilities that arise as a result of the ICT enabled interconnectivity. 29 Additionally, it highlights the need to respect others’ legitimate interests and recognise the possibility of one’s actions or inactions harming others given the pervasiveness of ICTs in societies. 30 The resolution adopted in 2004 in turn notes the role of ICTs in the promotion of socio-economic development and in the provision of goods and services. 31 The resolution adopted in 2009 emphasises that confidence and security in the use of ICTs are among ‘the main pillars of the information society’; 32 and it emphasises the increasing contribution of ICTs ‘to many of the essential functions of daily life, commerce and the provision of goods and services, research, innovation and entrepreneurship, and to the free flow of information among individuals and organizations,

27 Creation of a Global Culture of Cybersecurity (adopted by the UN General Assembly on 31 January 2003, UN Doc A/RES/57/239); Creation of a Global Culture of Cybersecurity and the Protection of Critical Information Infrastructures (adopted by the UN General Assembly on 30 January 2004, UN Doc A/RES/58/199); Creation of a Global Culture of Cybersecurity and the Protection of Critical Information Infrastructures (adopted by the UN General Assembly on 21 December 2009, UN Doc A/RES/64/211).
30 Creation of a Global Culture of Cybersecurity (adopted by the UN General Assembly on 31 January 2003, UN Doc A/RES/57/239), p. 3.
Governments, business and civil society'. The resolution also notes how the reliable functioning of ICT infrastructure and the integrity of information affect global welfare. Additionally, following the Edward Snowden revelations, the Third Committee (the Social, Cultural and Humanitarian Committee) has expressed a ‘deep concern’ about the negative impact of mass scale surveillance and data interception programs on human rights to privacy.

Finally, initially in 2004, the First Committee established a Group of Governmental Experts (GGE) to examine existing and potential threats from cyberspace. In the 2013 report the GGE affirmed the application of existing international law and UN Charter principles, noting that law is needed to ensure ‘an open, secure, peaceful and accessible ICT environment’. The report also concluded that state sovereignty applies to both the ‘ICT-related activities’ of states and to ‘their jurisdiction over ICT infrastructure within their territory’. It was also noted that the use of ICTs ‘has reshaped the international security environment’ and that, while ‘[t]hese technologies bring immense economic and social benefits; they can also be used for purposes that are inconsistent with international peace and security.’ In the 2015 report the GGE focused particularly on norms of behaviour for states in relation to their ICT activities. These included, for example, that states should not conduct or support ICT activities that cause damage to the critical infrastructure of other states.

Therefore, as illustrated by various resolutions by the UN General Assembly, it has been

---

34 *Creation of a Global Culture of Cybersecurity and the Protection of Critical Information Infrastructures* (adopted by the UN General Assembly on 21 December 2009, UN Doc A/RES/64/211), p 2.
recognised by the international community on the UN level that ICTs and information are becoming increasingly fundamental to the functioning and prosperity of modern societies.

Accordingly, states as industrial societies have used basic ICTs, such as telegraphic and radio technologies, to transmit data across borders since the nineteenth century. Also, through various international efforts, they have sought to regulate and secure global ICT infrastructures and information flows. Increasingly however, ICTs are not simply a means of communication but intrinsically intertwined into the fabric of modern society. The hallmark of ‘post-industrial’ or ‘information societies’ is that these societies are increasingly not just using ICTs, such as radios or telephones in communications, but instead becoming dependent on digital ICTs and on information as a resource. As Ugo Pagallo maintains:

whereas over the past centuries, human societies have used information and communication technology (ICT), but have been mainly dependent on technologies that revolve around energy and basic resources, today’s societies are increasingly dependent on ICT and, furthermore, on information as a vital resource. Essential functions of today’s societies, such as governmental services, transportation and communication systems, business processes or energy production and distribution networks, depend on the use of computer platforms.\footnote{Pagallo (2015a), p 409. Floridi describes these as ‘hyperhistorical’ societies – societies in which ‘ICTs and their data processing capabilities are the necessary condition for the maintenance and any further development of societal welfare, personal well-being, as well as overall flourishing.’ Floridi (2015a), p 52 (emphasis in original).}

With technological advancement and increasing digitalisation of essential societal functions, states have also become vulnerable to attacks on information through information. For example, the notion of critical infrastructure is defined within the context of the European Union (EU) as those assets or systems ‘essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people’\footnote{Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection [2008] OJ L 345/75, Article 2.} – essentially referring to physical infrastructure which is vital for the proper functioning of society. The term critical information infrastructure in turn is used to describe both the essential ICT infrastructures, and those that are essential for the operation of the aforementioned physical critical infrastructures.\footnote{Commission of the European Communities (2005) ‘Green Paper on a European Programme for Critical Infrastructure Protection’ COM (2005) 576 final, 17 November 2005, p 19 (emphasis added).} Accordingly, the proper functioning of the infrastructure of information societies is intertwined with ICTs, meaning states have also become vulnerable
to informational threats. A range of cyber attacks provide novel informational means through which to disrupt information systems or undermine the integrity of the information these systems rely upon. Distributed Denial of Service (DDoS) attacks for example, can flood a computer system with information and disrupt its operation, and malicious software such as computer viruses can be designed to alter information and undermine the proper operation of information systems. Therefore, as states are becoming increasingly reliant on ICTs, they are becoming vulnerable to information flows that are capable of harming them in new ways. Information is in effect flowing into how interstate uses of force are conceptualised, and thereby challenging traditional understandings of interstate violence, and the ability of law to regulate and contain interstate violence.

Section 2: International Law and the Containment of Violence

This section explores the relationship between international law and violence. It demonstrates how the containment of violence through international law is central to the UN Charter based international legal order. As such, it explores the tension between violence within the contemplation of positive law and violence that is outside the realm of law. In international law, this tension is evident in the law’s relationship with war and violence. Through international law, states have sought to contain the violence associated with warfare by limiting the authority to wage violence to the sovereign state, and by limiting the violence inherent in warfare through law. In the modern context, the prohibition on the use of force provides the doctrinal limitation on the most intense forms of violent coercion, and the modern means through which international law seeks to contain violence. Against this depiction of international law’s containment of violence, the following section will then demonstrate how cyber attacks are challenging this containment.

2.1 Violence, the State, and Law

Walter Benjamin distinguished between two forms of violence. He described one as lawmaking violence which refers to the violence evident in the establishment of every legal order. Law-preserving violence on the other hand refers to legal violence which is used to

43 Benjamin (2002), pp 241-244.
44 Benjamin (2002), pp 243, 248. According to Ari Hirvonen, Benjamin’s lawmaking (or law-positing or law-imposing) violence is violence that is not legal or illegal and provides the foundation or constitution of a legal order. It ‘points beyond itself in order to maintain itself.’ Hirvonen (2011), p 102.
preserve the legal order.\(^{45}\) He maintained that law has an interest in the monopoly of violence in order to preserve itself, as ‘violence, when not in the hands of the law, threatens it not by the ends that it may pursue but by its mere existence outside the law.’\(^{46}\) Also in the context of interstate relations, there is an implicit distinction between forms of violence that are part of the legal order and those forms that are external to it and hence considered outside the law. This is evident particularly in the classical realist image of war and its placement outside the confines of law. According to Michael Walzer for example, for classical realists:

> War is a world apart, where life itself is at stake, where human nature is reduced to its elemental forms, where self-interest and necessity prevail. Here men and women do what they must to save themselves and their communities, and morality and law have no place. *Inter arma silent leges*: in time of war the law is silent.\(^{47}\)

Interstate violence was therefore classically seen as taking place in a state of nature in which the law was silent. Martti Koskenniemi has described a similar imagery:

> For the classical realists, the founding violence of law – the violence which could not be encompassed by law because it was its precondition – was an act of physical force, sending in the military to occupy a territory or to overthrow (or uphold) a government, war, aggression, sovereignty: great moments of historical significance. These were the *a priori* on which the law was based and could not, therefore, be captured within law.\(^{48}\)

This tension between violence that is outside the law and the legal order, and violence that is captured by the law and within the legal order, is implicit in the general relationship between law and violence. Despite the various forms of violence that may often escape the law or in which the law is even implicit in, the central focus of international law is, as Koskenniemi highlights, the physical violence surrounding the military forces of states engaging in inherently territorial conflicts.\(^{49}\) As such, international law is particularly concerned with the violence associated with war and its containment through and within positive law.

---


\(^{46}\) Benjamin (2002), p 239.


\(^{49}\) For instance, in relation to the armed conflict in Kosovo, Koskenniemi notes how the ‘[o]bsessive talk about Kosovo makes invisible the extreme injustice of the system of global distribution of wealth, reducing it to the
In international law, the notion of violence is largely defined by specific legal vocabularies. For instance, the term ‘violence’ itself is often only mentioned in relation to illegitimate uses of force and hence contrasted to seemingly legitimate forms of violence such as ‘military offensives’. However, even on a personal level, the meaning of the notion of violence is debated. In this context violence is generally understood as direct intentional harm to a human being. Harm here can take various forms – from physical to psychological harm, or some form of deprivation. Despite general agreement on the core meaning of violence as, at least, direct intentional harm to human beings, there is a hesitance to extend the notion of violence beyond physical acts causing suffering or death to humans, to cover ‘violence against things’ for instance. In the international context, international humanitarian law is

sphere of the private, the unpolitical, the natural, the historically determined – just like war used to be – a ‘social’, ‘cultural’ or ‘economic’ condition of law which cannot be touched by law.’ Koskenniemi (2002), p 172 (emphasis in original). Myers McDougal and Florentino Feliciano in turn describe the minimisation of change by major coercion and violence as ‘the most fundamental policy projected by international law’, and the ‘law of war’ as the result of the global process to minimise coercion and violence. McDougal and Feliciano (1994), p xix, xxiv–xxv. Gina Heathcote also maintains that international law on the use of force is ‘the manifestation of the law/violence relationship within the international sphere’ (which she argues is a gendered discourse). Heathcote (2012), p 11.

50 Thomas (2011), p 1819-1821. Claire Thomas, for example, argues that the distinction between legitimate force and (illegitimate) violence is problematic as it ‘constructs a discourse of legitimacy around all state violence, and it hides the violence of state action.’ Thomas (2011), p 1821.

51 According to a dictionary definition, violence is ‘behaviour involving physical force intended to hurt, damage, or kill someone or something’. Stevenson (2010). In contrast, ‘non-violence’ is defined as ‘the use of peaceful means, not force, to bring about political or social change’. Stevenson (2010).

52 The World Health Organisation for instance defines violence as ‘[t]he intentional use of physical force or power, threatened or actual, against oneself, another person, or against a group or community, that either results in or has a high likelihood of resulting in injury, death, psychological harm, maldevelopment or deprivation.’ Krug et al (2002), p 5.

53 Coady (1986), p 4. In the debates on the meaning of violence, some argue for a broad scope considering structural injustices as a form of violence. Newton Garver for instance connects the idea of violence to the notion of ‘violation’, arguing that violence should be understood in terms of a person being violated, opposed to merely subject to force. Garver (1970), p 257. Johan Galtung also defines violence broadly, arguing that ‘violence is present when human beings are being influenced so that their actual somatic and mental realizations are below their potential realizations.’ Galtung (1969), p 168. However, his definition has been criticised for its excessive breadth, see Betz (1977), p 343. John Keane also criticises Galtung’s account, arguing it makes violence ‘virtually synonymous with all human failures to live happily, like angels, unburdened by the curse of politics, within a universe of ‘symbiotic, equitable relations among diverse partners’ held together by ‘cooperation, friendliness and love’.’ See Keane (2004), p 35. Some authors even raise the possibility that the destruction of things could constitute violence. Galtung for instance argues that this could be the case, at least where it involves the ‘destruction of something very dear to persons referred to as consumers or owners.’ Galtung (1969), p 170 (emphasis in original).

54 Keane (2004), pp 33-34. Keane defines violence as:

the more or less intended, direct but unwanted physical interference by groups and/or individuals with the bodies of others, who are consequently made to suffer a series of effects ranging from shock, speechlessness, mental torment, nightmares, bruises, scratches, swellings, or headaches through to broken bones, heart attacks, loss of body parts, or death.

Keane (2004), p 35. See also Keane (1996), pp 66-67. He maintains that it must have an embodied quality as it must ultimately affect the bodies of individuals. Keane (2004), pp 36-38.
arguably closely concerned with violence on a personal level, including a concern about violence towards civilian objects, and even violence towards the natural environment as it concerns the survival of individuals. On the other hand, the law on the use of force is aimed at containing the outbreak of violent interstate conflict. As will be shown, it embodies a particular understanding of what constitutes a prohibited form of interstate violence, and in seeking to limit the use of violence by states in their international relations, constitutes a relatively recent phenomenon in international law.

While the modern UN Charter prohibition on the use of force marks a shift away from the traditional ‘war’ vocabulary, from a historical perspective, it nonetheless marks a continuation of the containment of violence discourse evident in international law and thinking about international order. One of the central aims of the UN Charter system is the maintenance of international peace and security through the peaceful settlement of disputes and therefore the containment of the violence associated with war. Unlike previously when

55 Common Article 3 for instance prohibits ‘violence to life and person, in particular murder of all kinds, mutilation, cruel treatment and torture’ to various classes of people in and affected by armed conflict, see Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, opened for signature, opened for signature 12 August 1949, [1958] ATS 21 (entered into force 21 October 1950), Article 3. Antonio Cassese has described international humanitarian law as designed to constrain the violence unleashed by war from spilling over its legal limits. Cassese (1988), p 108.


58 During the nineteenth and early twentieth centuries war was regarded as the sovereign prerogative and an essential element of sovereignty, see Dinstein (2001), p 71. The early twentieth century saw a shift towards a more restricted right to war however, as reflected in the attempts to restrict the right to war in the Covenant of the League of Nations, opened for signature 28 June 1919, [1920] ATS 1 (entered into force 10 January 1920), Article 12. While the Covenant did not seek to abolish the right to war completely, this was the aim of the League in implementing the General Treaty for the Renunciation of War as an Instrument of National Policy (Kellogg-Briand Pact), opened for signature 27 August 1928, [1929] ATS 1 (entered into force 24 July 1929), Article 1. See also Dinstein (2001), p 77. Apart from a limited number of exceptions in this treaty, the aim was to prohibit all uses of armed force and thus place the right to engage in war ‘outside the legal competence of states.’ Brownlie (1963), p 91. With the UN Charter instead restraining the use of ‘force’, even the word ‘war’ was eliminated from the discourse – thus, as Kennedy notes, the ‘law of war’ became the ‘law of force’. Kennedy (2006), p 78.

59 Originating from early Greek and Roman scholars and statesmen, through the medieval theologians and early modern scholastics to modern international law scholars, these debates and the frameworks of thinking about the just causes of war and the permitted forms of violence within war have varied. For an overview of the historical development of just war theory in relation to the legality of war, see Brownlie (1963), pp 3-17; Dinstein (2001), pp 59-68. Anthony Anghie notes that the questions of who can wage war, when it can be waged, what are the limits of warfare, and when is a war just – are among the ‘traditional questions’ international lawyers are still occupied with today, just as Francisco de Vitoria was in the early sixteenth century. Anghie (1996), p 328.

war was considered a legitimate form of statecraft under international law, the UN Charter era is characterised by a general prohibition on the use of force. As such, in contrast to the classical realist depiction of war as a form of legally unfettered violence within a state of nature, the modern idea of war is more akin to orderly duel.\textsuperscript{61} Now war, or armed conflict between states,\textsuperscript{62} while temporally deviating from periods of peace, occurs in a legal space.\textsuperscript{63} Both the entry into war and the conduct of warfare itself are heavily regulated by law. The modern institution of war, according to Hedley Bull for instance, is part of certain rules of coexistence that allow states to limit violence with the aim of maintaining international order.\textsuperscript{64} According to Bull, these rules seek to confine legitimate violence exclusively to the state by confining legitimate violence to a particular kind of violence called ‘war’, and treating war as violence that is waged on the authority of a sovereign state. Furthermore, the rules seek to limit the causes or purposes for which a sovereign state can legitimately begin a war, … the manner in which sovereign states conduct war, … [and] restrict the geographical spread of a war.\textsuperscript{65}

Bull’s account demonstrates how one of the central aims of international law is to contain violence. He also notes how the modern concept of war came about from a process of limiting and containing violence, opposed to its historical alternative of ‘more ubiquitous violence.’\textsuperscript{66} Therefore, international law has sought to capture the violence inherent in war in particular, and bring it under the control of law.

\textsuperscript{61} Clausewitz (1968), pp 101-102.
\textsuperscript{62} According to Oppenheim’s widely used definition, ‘[w]ar is a contention between two or more States through their armed forces, for the purpose of overpowering each other and imposing such conditions of peace as the victor pleases.’ Oppenheim (1952), p 202, cited in Dinstein (2001), p 4.
\textsuperscript{63} David Kennedy for instance maintains that:

\begin{quote}
When we think of war as sharply distinct from peace, it is easy to imagine it also as outside of law. War is often the exception to the routine legal arrangements of peacetime; contracts, for example, routinely exempt acts of war along with “acts of God.” If we pause to think about the law relevant to war, we are likely to focus on international rules designed to limit the incidence of warfare, from the ancient “just war” tradition, to the institutional machinery set in place by the United Nations Charter to “save succeeding generations from the scourge of war.” Or the many disarmament treaties limiting the use or availability of the most heinous weapons—exploding bullets, gas, chemical, or nuclear weapons. We are likely to think of these rules as coming from “outside” of war, limiting and restricting the military. We think of international law as a broadly humanist and civilising force, standing back from war, judging it as just or unjust, while offering itself as a code of conduct to limit violence on the battlefield.
\end{quote}

\textsuperscript{64} Kennedy (2006), pp 5-6.
\textsuperscript{65} Bull notes that ‘[m]ost states at most times pay some respect to the basic rules of coexistence in international society, such as mutual respect for sovereignty, the rule that agreements should be kept, and rules limiting resort to violence.’ Bull (2002), p 40.
\textsuperscript{66} Bull (2002), p 66.
\textsuperscript{67} Bull (2002), p 179.
As Bull’s account also highlights, the sovereign state is also central to international law’s containment of violence. The classic Hobbesian image of the state as a Leviathan is one of an ‘artificial man’ whose soul comes from its sovereignty. The state is often described as an anthropomorphic entity, and its territorial ‘body’ is conceptualised as a container of modern society which separates its internal or domestic affairs from its external or foreign affairs. It is a territorially bound unit with supreme authority within its boundaries, and this authority is also recognised externally by other states. Internally, the state’s sovereignty is manifested in its exclusive jurisdiction over its internal matters – its governing authority and resulting effective control of everything including legislation, taxation, immigration, citizenship, and law enforcement. Externally, this authority is recognised by other states and embodied in the international legal obligation of non-intervention. To maintain or defend its supreme authority in these dimensions, states hold a monopoly of legitimate violence. Internally, this monopoly manifests in the legitimate authority to enforce the law and maintain order, and externally the state holds the sole legal capacity to engage in violence in the form of war. Therefore, the state is classically viewed as a legal and territorial entity effectively controlling law and violence internally, and being the sole entity capable of legitimately engaging in violence internationally.

68 This image pervades literature on the state as the state is depicted as an individual ‘actor’ or ‘person’ with an identity and interests that holds rights and obligations. For instance, according to Erik Ringmar, the state ‘is almost invariably talked about in anthropomorphic terms. It is seen as an ‘actor’ or a ‘person’; it is a ‘someone’ or a ‘subject’ to whom intentions, memories, rights and obligations are attached.’ Ringmar (1996), p 443. Similarly, Alexander Wendt argues that ‘state personhood’ pervades social science and international relations literature – states are ‘actors’ or ‘persons’ to whom properties associated with human beings, such as ‘rationality, identities, interests, [and] beliefs’, are attributed to. Wendt (2004), p 289.
69 Anthony Giddens for instance describes the state as ‘the pre-eminent form of power container, as a territorially bounded (although internally highly regionalized) administrative unity.’ Giddens (1985), p 13. See also Taylor (1994). According to John Agnew, the traditional state centred account of the spatiality of power, rests on three assumptions, namely that ‘modern state sovereignty requires clearly bounded territorial spaces’; that there is a clear distinction between domestic and foreign affairs due to the view ‘that states are akin to individual persons struggling for wealth and power in a hostile world’; and that ‘the territorial state acts as the geographical ‘container’ of modern society.’ Agnew (1998), p 51.
70 See Little (2005), pp 768-769.
71 Crawford (2012), pp 120-121.
72 Little (2005), p 769.
73 According to Max Weber, ‘a state is a human community that (successfully) claims the monopoly of the legitimate use of physical force within a given territory … The state is considered the sole source of the ‘right’ to use violence.’ Gerth and Mills (2009), p 78 (emphasis in original). See also Kalberg (2005), p 222; Turner (2002), p 198.
74 According to Richard Little, this is how the state is understood in the classical nineteenth and twentieth century context, in contrast to earlier times when non-state actors such as mercenaries and pirates were mainly responsible for the violence that took place internationally. Little (2005), p 773. See also Thomson (1996).
This imagery of the state as a person or actor is also evident in international law. States are, according to Antonio Cassese for example, ‘the *dramatis personae* (the characters of the play) on the international scene’.

To exist as a state, an entity must have a permanent human population, a defined natural (opposed to purely artificial or virtual) territory, a government, and the capacity to enter into relations with other states. Without these features, an entity is generally not considered a state. Territory is a particularly important element of statehood and it goes to the very essence of the state – both in terms of its existence and as the dimension within which states ‘perform’ their activities. Additionally, for the purposes of international law, the state is deemed a single and largely coherent entity. For instance, under the laws of state responsibility, regardless of the internal makeup of the state, the entire state as an entity is deemed responsible for the conduct of any of its ‘organs’ that is deemed internationally wrongful. As such, the law conceptualises the state as a fixed territorial entity with sovereignty.

Given their sovereignty, states are entitled to be free from interference by other equally sovereign states. Here the legal principles of non-intervention and non-use of force are central to the containment of violence within the UN Charter system. The non-intervention principle embodies the idea that states should be free to make their own choices

---

75 Cassese (2005), p 71. He also describes how insurgents ‘are born from a wound in the body of a particular State.’ Cassese (2005), p 71.


77 For example, entities located solely on artificial islands and therefore without natural territory have not been considered as states, because ‘...territory must consist in a natural segment of the earth’s surface’, see *Re Duchy of Sealand* (1978) 80 ILR 683 at 685.

78 See Cassese (2005), p 81. He writes that:

Most activities performed by the primary subjects of the world community, States, take place within a geographic area. Territory is crucial not only to the very existence of States (a State without territorial basis, however tiny it may be, is inconceivable). Territory also constitutes the dimension within which States employ their major activities.


The conduct of any State organ shall be considered an act of that State under international law, whether the organ exercises legislative, executive, judicial or any other functions, whatever position it holds in the organization of the State, and whatever its character as an organ of the central government or of a territorial unit of the State.

According to Cassese, this is reflective of the primitive nature of the international community where the ‘archaic concept of collective responsibility still prevails ... [as it is the whole State that incurs responsibility and which therefore has to take all the required remedial measures.]’ Cassese (2005), p 241.

80 For example, Eve Darian-Smith notes how in traditional scholarship on the state more generally, ‘[n]ation-states are interpreted as continuing to function as relatively fixed political and territorial entities against which non-state actors (and things) and their relationships to places, properties, homelands, and sovereignties (however defined) are posited.’ Darian-Smith (2013), p 179.
in relation to their political, social, economic and cultural system, and foreign policy.\(^81\) Other states should not, for instance through economic means, coerce them. The non-intervention principle thus aims to protect states from coercive interference by other states. As such, when the activities of a state rise above mere espionage or diplomatic pressure that may infringe on another state’s sovereignty, and instead aim to affect the state’s freedom in making the choices ‘which must remain free ones’,\(^82\) then those actions are regarded as unlawful and in breach of the non-intervention principle. The non-use of force principle on the other hand is considered as ‘the very cornerstone of the human effort to promote peace in a world torn by strife.’\(^83\) It seeks to prohibit those forms of coercion that, while technically also breaching the non-intervention principle, rise to a higher threshold. It essentially prohibits states from using more intense forms of coercion, such as the use of armed force, in their international relations.

The forms of coercion and violence captured by these legal principles are often conceptualised on a spectrum of intensity. Rosalyn Higgins for example argues that military force or intervention is at one end of the spectrum, whereas ‘any interference at all’ at the other end.\(^84\) Similarly, Myers McDougal and Florentino Feliciano distinguish between low-level coercion that ‘includes all coercion not accelerated to the levels of intensity and magnitude that signal impermissible coercion’, from the forms of ‘coercion of relatively great scope and intensity, including the most intense and extensive violence’.\(^85\) Accordingly, the most intense forms of violent coercion are generally conceptualised as uses of force, whereas the less intense measures or forms interference below the threshold only constitute breaches of the non-intervention principle or the sovereignty of a state. As will be shown in chapter 4, in the debates about the threshold distinction between these principles, the more intense forms of coercion involving harm to human beings or damage to physical objects are seen to be captured by the non-use of force principle as they affect the conceptual ‘body’ of the state. On the other hand, those forms of coercion below this threshold are effectively

\(^82\) Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v United States of America) (Merits) (1986) ICJ Reports 14 at 108 (para 205).
\(^83\) Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v United States of America) (Merits) (1986) ICJ Reports 14, at 153 (separate opinion of President Nagendra Singh).
\(^84\) Rosalyn Higgins maintains that intervention concerns a spectrum of activities, ranging ‘from the notion of any interference at all in the state’s affairs at the one end, to the concept of military intervention at the other.’ Higgins (2009), p 273.
\(^85\) McDougal and Feliciano (1994), p 207.
conceptualised as forms of non-violence that only affect the ‘personality of the state’.  

As such, the notion of ‘force’ in this context reflects an extension of the general core understanding of violence as ‘direct intentional acts of harm’, to ‘direct (or indirect) intentional acts of harm to a state’. Harm in this context generally requires some form of injury to humans or damage to physical objects for the law to be capable of recognising it as a form of prohibited interstate violence. Therefore, the non-use of force and non-intervention principles are central to modern international law’s containment of violence, and consequently form part of the effort by states to contain violence through and within the law.

2.2 Technology

In addition to the conceptual containment of violence within the confines of law, states have also sought to contain or control weapons technologies as the instruments of violence. Generally, and as a hallmark of modernity, technology is regarded in instrumental terms as a means through which deadly conflict can be waged and through which men can dominate nature. Simultaneously, given the potentially excessive violence that can be inflicted on human beings with technological means (from the crossbow to explosive bullets and nuclear weapons), technology itself is something that must be contained, and law is seen as the mechanism through which to do so. For example, through various arms control treaties such as the Treaty on the Non-Proliferation of Nuclear Weapons, the law seeks to contain and control the development, spread and deployment of various weapons technologies. Again the sovereign state is central to this effort, particularly given the resource intensive nature of these weapons development projects, and because international agreements to prohibit or limit these technologies are dependent on state consent.

As such, the law reflects the idea that to maintain international order, states should retain a monopoly over the technological means of violence – only state actors should be in possession of such weapons, and efforts by

---

86 See the Declaration on Principles of International Law Concerning Friendly Relations and Co-operation among States in Accordance with the Charter of the United Nations (adopted by the UN General Assembly on 24 October 1970, UN Doc A/RES/2625(XXV)).
87 As will be discussed in chapter 4, a use of force may also be ‘indirect’ according to the ICJ in Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America) (Merits) (1986) ICJ Reports 14.
89 For example, as the ICJ in Nicaragua v USA noted in relation to the spread of armaments and the militarisation of Nicaragua, ‘in international law there are no rules, other than such rules as may be accepted by the State concerned, by treaty or otherwise, whereby the level of armaments of a sovereign State can be limited, and this principle is valid for all States without exception.’ Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America) (Merits) (1986) ICJ Reports 14 at 135 (para 269).
non-state actors (from criminals to terrorist organisations) to obtain these weapons should be restricted to ensure international peace and security.

In addition to the role of states in limiting military weapons technologies, they have often also been the main drivers behind the development of military and related technologies. A key technological development which started as a military and research project was the development of what is now the Internet. The Internet’s development can be traced to the Cold War superpower rivalry and the potential for annihilation linked to the concern of the use of nuclear weapons technologies during the time. Communication during, or in the advent of, a nuclear war was a problem that both the military and the scientific community were concerned with. This, as well as the funding for research and development obtained in the context of the superpower rivalry and space race, pushed the efforts to develop technologies enabling digital communication through networks.\(^{90}\) Now cyberspace has become recognised in the military context as the fifth, virtual domain of warfare, alongside the physical land, sea, air, and outer-space domains.\(^{91}\) In many ways this is recognition of the increasing reliance of modern states and also militaries on ICTs, and the consequent vulnerabilities and opportunities this presents. The development and even deployment of various cyber weapons and other cyber enabled activities – from widespread information collection programs to sophisticated cyber attacks causing material damage to computer hardware – demonstrates that cyberspace has expanded the means and spaces in which states can engage in politics by other means. Hence what began partially as a need to develop communication methods in the context of the Cold War, now provides new possibilities and vulnerabilities, and hence new avenues for interstate conflict such as through the use of cyber attacks.

To summarise, the containment of violence is central to international law – the authority to wage violence is limited to the sovereign state, and warfare between sovereign states is limited by legal principles that flow from state sovereignty. Within the UN Charter international legal order, the violence associated with warfare, while conceptually outside the

---

\(^{90}\) See Bing (2009), pp 8-12, 20. Jon Bing notes that:

> It is often said that the Internet originated from the attempts of the US Department of Defense to develop a network that would survive an atomic attack … [though] this is a somewhat inaccurate part of cyberspace lore. Yet there is a kernel of truth in it, that kernel being Paul Baran and his fear of the Cold War blossoming into a very hot one. On account of that fear, he designed a robust network that would ensure the Strategic Air Command contact with the Launch Control Facilities for shooting the intercontinental ballistic missiles from their underground silos.

Bing (2009), p 12.

\(^{91}\) Clarke and Knake (2010), pp 44-47.
realm of law previously, is sought to be contained by law. In this context, the prohibition on
the use of force serves as a doctrinal limitation on the most intense forms of violent coercion.
Additionally, the technological dimension to international law’s containment of violence sees
technology as a means through which violence can be inflicted. As such, the law regards
technology as something that must be controlled in order to contain violence. However, as the
following section will demonstrate, cyber attacks are challenging the traditional
understanding of violence embodied in the law and therefore challenging international law’s
containment of violence.

Section 3: Cyber Attacks and the Containment of Violence

Cyber attacks are commonly defined as deliberate computer enabled actions used ‘to alter,
disrupt, deceive, degrade, or destroy adversary computer systems or networks or the
information and/or programs resident in or transiting these systems or networks.’92 As hostile
information flows, cyber attacks seek to compromise computer security in one or more ways
by undermining the integrity of information, undermining the operation of computer systems,
and/or disrupting the flow of information within a network.93 Like interstate coercion, cyber
attacks can be understood on a spectrum of intensity. At the lower end of this spectrum are
those generally termed as information collection operations, cyber exploitations or cyber
espionage – low intensity cyber attacks that involve unauthorised access to information and
degrade the integrity of information, for instance by undermining its sensitive or confidential
nature. At the higher end of this spectrum are cyber attacks that are capable of causing
material effects such as the destruction of computer hardware. In the context of states using
cyber attacks against other states in their international relations, the lower intensity forms of
cyber attacks, while questionable, are often not specifically prohibited by international law
and therefore regarded as permitted.94 In contrast, the more intense forms of cyber attacks

93 Herman Tavani, for example, describes the three dimensions of computer security as data security, system
security, and network security. Data security refers to ensuring the integrity of information by protecting it
against unauthorised access; system security refers to protecting a computer system’s resources (its software and
hardware); and network security refers to protecting computer networks (such as the Internet) from threats
94 As mentioned, this is the principle from SS ‘Lotus’ (France v Turkey) (Judgment) [1927] PCIJ (series A) No
10. Michael Schmitt for example writes that the revelations by Edward Snowden about the US National Security
Agency’s information collection program, ‘illustrates the international community’s unease with cyber
operations that target other states or their citizens, even when … perhaps lawful under current understandings of
international law.’ Schmitt (2014), p 276. This ‘unease’ is also reflected by the ‘deep concerns’ raised in recent
UN General Assembly resolutions about the impact of these mass surveillance programs on human rights, see
that cause physical destruction are more likely to constitute a form of ‘force’ that states are expressly prohibited from using in their international relations.\textsuperscript{95}

3.1 The Novel Nature of Cyber Warfare

The use of cyber attacks and therefore engaging in cyber warfare is only possible within the technological context of ICT driven societies.\textsuperscript{96} Cyber warfare however, is not simply a new means of engaging in traditional warfare that existing law is concerned with containing.\textsuperscript{97} Instead, cyber warfare is ontologically different – particularly in relation to the entities through which it is waged, the environment in which it is waged, and the harm or forms of violence that characterise it. Instead of human agents engaging in conflicts with kinetic weapons in physical environments that results in injury or death to humans, or damage or destruction of physical property – cyber warfare involves artificial agents engaging in conflicts in virtual environments that may or may not result in similar forms of harm. Due to these characteristics what arises is an ontological gap between the laws regulating existing warfare and cyber warfare.\textsuperscript{98} In other words, there is a disparity between cyber warfare and

\textit{The Right to Privacy in the Digital Age} (adopted by the UN General Assembly on 18 December 2013, UN Doc A/RES/68/167), p 2. However, the United States has been reported to be more concerned with economic espionage and to some degree condoning political espionage, see Parameswaran, ‘Time for the US to Punish China in Cyberspace?’, The Diplomat, 20 August 2015. Shackelford also notes how ‘both outer space and cyberspace are domains in which intelligence gathering has been widely tolerated, even though the outcry has been greater in the case of cyber espionage than orbital reconnaissance.’ Shackelford (2014), p 274 (citations omitted).

95 These issues will be examined in more detail in chapter 4.

96 A useful descriptive (opposed to legal) definition of cyber war comes from Richard Clarke and Robert Knake, who define it as referring to ‘actions by a nation-state to penetrate another nation’s computers or networks for the purposes of causing damage or disruption.’ Clarke and Knake (2010), p 6.

97 In relation to cyber warfare and the complications that arise in the classification of conflicts into those between states, and internal conflicts, Schmitt maintains that:

\begin{quote}
Cyber operations have the potential for producing vast societal and economic disruption without causing the physical damage typically associated with armed conflict. They are also inherently transborder, thereby frustrating any approach to classification based on geographical factors. Moreover, massive attacks can be launched by a single individual or by a group that is organized entirely on-line. This is in sharp contrast to traditional warfare, which depends on either the involvement of a State’s armed forces or that of a group capable of mounting typical military operations.
\end{quote}


98 Taddeo argues that there is an ‘ontological hiatus’ between traditional warfare and information warfare – the former involves ‘human beings and physical objects’ while the latter ‘involves artificial and non-physical entities alongside human beings and physical objects’. Taddeo (2016), p 216. This ontological hiatus or gap affects just war theory that underpins the law on the use of force, as it ‘rests on an anthropocentric ontology, i.e. moral discourse is solely concerned with respect for human rights and disregards all non-human entities’. Taddeo (2016), p 216. Dipert also notes similar ontological problems, see Dipert (2010), pp 399-400; Dipert (2013), p 36.
international law’s existing containment of violence. Summarising the novelties of cyber warfare as a form of ‘information warfare,’ Mariarosaria Taddeo defines the latter as:

the use of ICTs within an offensive or defensive military strategy endorsed by a state and aiming at the immediate disruption or control of the enemy’s resources, and which is waged within the informational environment, with agents and targets ranging both on the physical and non-physical domains and whose level of violence may vary upon circumstances.\(^{99}\)

While information warfare in this definition incorporates various forms of modern conflict engaged through drones, robots and technologically enhanced soldiers for example, cyber warfare is a particular form of information warfare involving the use of cyber attacks. The novelties of this form of warfare, as highlighted by Taddeo’s account, involve: 1) the entities waging cyber warfare, 2) the environment in which it takes place, and 3) the forms of harm or violence inflicted through cyber warfare.

### 3.1.1 Entities

Unlike traditional warfare waged through human agents, cyber warfare involves a wider ontological range of agents. Taddeo highlights how the ontological status of agents involved in waging information warfare include both ‘artificial agents, such as viruses, drones and robots for example, and human agents.’\(^{101}\) Thus in contrast to traditional warfare waged by human agents with technological artefacts against other human beings or physical objects, cyber warfare in particular involves both human and artificial entities. Further, while traditional warfare is waged through military personnel, skills and techniques; the people and skills required for cyber warfare are not military specific which results in a blurring of ‘the distinctions between civil society and military organisation.’\(^{102}\) Hence the agents involved in waging cyber warfare are not only human, but also artificial. For example, malicious computer software such as viruses and worms can be designed to attack computer systems and networks. Once created and propagated, these artificial entities self-replicate and operate

\(^{99}\) This is in contrast to the usual military definition of information warfare, which mainly focuses on a range of methods that are used to manipulate or deceive adversaries through information, or deny them access to information during conflict. Libicki (1995), pp x-xi. See also Barkham (2001), pp 60-62. Taddeo uses this term to highlight the essentially informational nature of cyber warfare – hence locating it within the other means of ICT enabled warfare. See Taddeo (2012), p 114.

\(^{101}\) Taddeo (2012), p 114.

\(^{102}\) Taddeo (2012), p 114.
with a degree of autonomy as they are able to scan for potential targets, select them based on their potential success, self-replicate and spread into those targets, and deliver whatever payload they are designed for.\textsuperscript{103}

3.1.2 Environment

Land, sea, air and outer-space constitute the four physical domains of warfare. The ‘fifth domain’ of cyberspace however, is an entirely artificial, man-made virtual space. Even though the notion of space is used metaphorically in this context, cyber warfare is waged in and through the virtual environment of cyberspace. For instance, the US Department of Defense defines cyberspace as a ‘global domain within the information environment’ that is made up of the various networks, the data residing therein and includes computer systems and processors.\textsuperscript{104} The ITU instead uses the broader term ‘cyber environment’ to refer to the various users, networks, devices, programs, processes and information that is directly or indirectly connected to networks.\textsuperscript{105} In both cases cyberspace is conceptualised as an artificial environment that is created by human technologies that enable the operation of virtual networks such as the Internet. Indeed, with the increasing reliance of states on ICTs for their proper functioning, cyber warfare is not limited to a purely virtual environment. Instead, cyber warfare can be waged in both physical and virtual domains, as digital ‘cyber weapons’ can be used to affect both informational objects and also physical objects, or individuals in the physical domain.\textsuperscript{106} Given its artificial nature, even cyberspace itself as an environment can be the target of cyber warfare.\textsuperscript{107} As mentioned above, various UN General Assembly resolutions also highlight the dependence of states on ICT infrastructure, and how the wellbeing and prosperity of societies is increasingly vulnerable to threats from cyberspace. As such, while cyberspace constitutes a virtual environment, it increasingly intersects and converges with the physical environment given the integration of ICTs into everything from

\textsuperscript{103} Chen et al (2006), p 54-55. The term ‘payload’ refers broadly to ‘the things that can be done once a vulnerability has been exploited.’ Owens et al (2009), p 88. The payload of a computer worm, for example, can be ‘virtually anything’ and does not need to be destructive. See Chen et al (2006), p 55.
\textsuperscript{104} Joint Staff (2010), p 58.
\textsuperscript{105} International Telecommunications Union (2008), p 2.
\textsuperscript{106} Taddeo (2012), p 113.
\textsuperscript{107} Kanuck for example writes that: even more problematic than information warfare against data is an attack against the medium itself. While it may be initially difficult to fathom an assault on an enemy’s airspace that would render it useless, that is, in essence, the very goal of electronic warfare, which involves jamming frequencies of the electromagnetic spectrum or incapacitating computer systems. Kanuck (1996), p 288. See also Chen et al (2006), p 48.
critical infrastructure, traffic control, to military equipment and communications.\footnote{108 See Jaeger (2006), pp 22-23.} Accordingly, unlike traditional warfare waged in the physical land, sea, air and outer-space domains, cyber warfare is waged in and through virtual environments that are increasingly embedded into objects in the physical environment.

### 3.1.3 Harm and violence

In addition to the difference between cyber warfare and traditional warfare in relation to the agents waging warfare and where warfare is waged, perhaps the most important difference is the harm associated with cyber warfare – the forms of violence associated with the use of cyber attacks. Cyber attacks are generally not viewed as a form of violence. For instance, those adopting a conventional view of violence, essentially as direct intentional acts of harm towards human beings, argue that cyber attacks ‘cannot be sensibly understood as a form of violent action’ as any potentially violent force is indirect.\footnote{109 Rid (2013), p 12.} As such, cyber attacks by themselves cannot harm a human being like energy (such as heat or a laser), or a chemical or biological agent directed towards (or being exposed to) a human can.\footnote{110 Thomas Rid maintains that any such violence is indirect, requiring the code to unleash the pre-existing violent potential of the target system – for instance causing a nuclear reactor to explode or emit radiation, a dam to unleash large amounts of water, or a pacemaker to be disrupted. Rid (2013), p 13. Some adopt a broader view of violence, for instance a 2015 report by the UN Broadband Commission for Digital Development considers the notion of ‘cyber violence’ against women to capture the various forms of gender-based violence that are exacerbated or made possible by the Internet. In this report, cyber violence captures a range of activities that occur in or through cyberspace, including online harassment, surveillance or tracking of women, and public humiliation. See UN Broadband Commission for Digital Development (2015), pp 21-22.} This view of violence is echoed in commentary on cyber attacks in relation to international humanitarian law, where cyber attacks are considered in terms of their violent consequences and not simply by their potentially violent nature.\footnote{111 The Tallinn Manual’s Group of Experts examine the notion of ‘cyber attack’ in the context of the law of armed conflict (international humanitarian law). Rule 30 provides that a cyber attack is a cyber operation ‘that is reasonably expected to cause injury or death to persons or damage or destruction to objects.’ Rule 30, Schmitt (2013b), p 106. The commentary then distinguishes between the use of violence against targets and non-violent operations such as cyber espionage, with the former constituting violence but not the latter. The Group of Experts go on to define ‘acts of violence’ as generally those releasing kinetic force with the exception of non-kinetic ‘chemical, biological, or radiological’ means also constituting attacks. They note that the crux lies in the effects caused. Hence an attack is defined by its consequences and not its nature: ‘violence’ must be considered in the sense of violent consequences and is not limited to violent acts.’ Commentary to Rule 30, Schmitt (2013b), pp 106-107.} Also by the traditional accounts of the law regulating interstate violence, the notion of violence is closely connected to the physical destruction and death associated with warfare. According to Durante, this view of violence also pervades political theory: ‘[v]iolence is anthropologically founded: human beings are intrinsically violent, and
violence is understood in kinetic terms as physical violence.112 Cyber warfare however, challenges this conceptualisation of violence, as it less often involves physical violence but instead forms of exploitation and disruption, or forms of ‘informational violence.’113

Therefore, while traditional warfare is characterised by kinetic attacks, death of human beings and destruction of physical property, cyber warfare does not necessarily have these characteristics.114 Cyber warfare primarily affects information meaning the effect of cyber attacks and the harm that they cause is not necessarily to human beings or physical objects. Randall Dipert for instance notes the novelty of cyber warfare, and that unlike traditional (or even nuclear) weapons, ‘many cyberattacks will not be lethal and will not even result in permanent damage to physical objects.’115 A cyber attack instead involves the disruption of an information processing system rather than the killing of human beings or the permanent destruction of physical objects. It crucially involves harm to the functioning of systems but not necessarily with permanent (hardware) destruction.116

While it is possible to inflict physical harm or destruction through cyber warfare, more often cyber attacks are only disruptive and any harm they cause is to non-physical entities such as the software allowing the system to function.117 This means that in contrast to the death and destruction associated with traditional warfare, the harm and consequent violence inherent in cyber warfare is not necessarily physical and possibly only affects virtual entities in a virtual environment. In essence, the inherently anthropocentric and materialist understanding of violence associated with warfare is not characteristic of cyber warfare.

112 Durante (2014), p 8. Durante also investigates the notion of violence in order to consider how cyber war is different from traditional war and how force is conventionally understood, see Durante (2014), pp 4-11.
113 Though sometimes cyber warfare can be used as a precursor to or an enabler of physical attacks, such as in the case of the suspected Israeli airstrike on a Syrian nuclear facility, where it is believed that Israel first used cyber attacks to disable Syrian air defence radars. See Clarke and Knake (2010), pp 6-8. The notion of informational violence will be discussed in section four of this chapter.
114 According to Durante, ‘[w]ar is no longer based only or even mostly on kinetic armed attacks but also on political, economic, ideological and informational strategies intended to exploit someone else’s informational resources.’ Durante (2014), pp 1-2. Taddeo similarly writes that existing laws on warfare focus ‘on violent warfare, bloodshed and physical damage’ – and while essential characteristics of kinetic warfare, they are not peculiar of information or cyber warfare. Taddeo (2016), p 217.
117 However, as Taddeo notes, cyber warfare is not simply ‘a ‘non-sanguinary, cheap and less military-based version of classic warfare’ as it too can be ‘as bloody and violent as traditional warfare’. Taddeo (2012), p 112.
As such, cyber warfare challenges the traditional understandings of violence inherent in kinetic warfare, and consequently the ontology underpinning of the law regulating interstate violence.\textsuperscript{118} It is argued that this gives rise to a new tension between law and forms of ‘informational violence’ that the law is incapable of recognising. As a result of this ontological gap between traditional warfare and cyber warfare, as will be demonstrated in chapter 4, the law embodies an ontologically constrained view of violence which is particularly evident in existing legal analyses of cyber attacks and the use of force threshold. Consequently, given the law’s ontological constraints, especially non-material cyber attacks – that is, cyber attacks with disruptive or purely informational effects – largely escape the law’s conceptual containment of violence. Therefore, as the following section will demonstrate, an informational approach offers a means through which law’s ontological constraints can be overcome. This enables recognition of other forms of violence that are capable of harming the state, such as informational violence, which currently escape the law’s containment of violence. On a more conceptual level, it also offers a way in which to see cyber attacks as a form of violence against the state as an information entity.

Section 4: An Informational Approach

As demonstrated in chapter 2, information ethics provides a conceptual framework based on an informational ontology that is concerned with the wellbeing of the infosphere. Others have also drawn on information ethics to consider some of the ethical issues surrounding cyber warfare. For example, both Taddeo and Pagallo have considered the traditional just war principles in the context of the four moral laws of information ethics to develop their respective perspectives on the morality of cyber warfare.\textsuperscript{119} The focus here and in the following chapters however, is not on whether cyber attacks are morally permitted or reprehensible pursuant to the moral laws of information ethics. Instead, an informational

\textsuperscript{118} Dipert for example also notes how ‘cyberwarfare involves aspects of damage or harm that are typically not addressed by law, such as harm to the functioning of information and other systems that might not harm physical objects or persons.’ Dipert (2010), p 395.

\textsuperscript{119} These authors mainly adopt the four principles of information ethics and merge them with just war principles to consider the legitimacy of the circumstances in which, cyber attacks for instance, can be used. Taddeo for example, drawing on the four moral laws of information ethics and the notion of ontological equality, maintains that the moral evaluation of cyber warfare needs to consider the consequences of a cyber attack for both humans and the information infrastructure that is being disrupted. Therefore, she argues that non-physical harm to the infosphere can be considered in conjunction with the harm to physical entities. See Taddeo (2016), pp 221-222. Pagallo similarly argues that pursuant to the ontological equality principle, the lawfulness of not merely physical also virtual force can be determined pursuant to the laws of information ethics. See Pagallo (2015a), pp 416-419.
approach is used to reconceptualise the notion of violence in relation to cyber attacks. This involves rethinking the harm caused by cyber attacks in terms of the increases in entropy they produce, and a reconceptualisation of the state as the entity subject to violence. Therefore, drawing on information ethics, it is argued that an informational approach offers a means to reconfigure the law’s ontological constraints. This enables recognition of a broader spectrum of violence that states can be subject to and which can undermine the law’s central concern with the containment of violence.

Accordingly, this section offers an informational reconceptualisation of the state, violence and law. First, the state is described as an information entity. It is depicted as a dynamic entity that continuously receives, processes and communicates information from and in the physical and virtual environments (the infosphere) in which it is situated. It is described as an entity that is constituted by its internal components (various sub-entities and sub-systems), and configured by the protocols that give it coherence as an entity. The state entity is therefore conceptualised as an information system, and the purpose of this entity is to care for and protect the wellbeing of its region of the infosphere. Following this, this section will consider cyber attacks as a form of violence causing entropy and undermining the very essence of the state entity. Finally, this section considers international law as providing the protocols according to which state entities operate within the international system.

4.1 State

Viewed informationally, the state is a non-static and continuously changing entity. Given the nature of global information infrastructures and information flows, the state entity continuously receives information from other entities. From the data flows stemming from individuals’ use of the Internet, financial data flows into banks and other corporations within

---

120 As will be discussed below, Floridi describes the state as a multiagent system or ‘MAS’ among other similar entities such as corporations, terrorist organisations and international organisations (see Floridi (2014), pp 175-180). However, as this thesis explores international law on the use of force (an area of law that applies primarily to states, opposed to non-state actors), the focus will be on the harm caused by cyber attacks to state entities. In other words, the ‘level of abstraction’ used in this thesis is set at the level of public international law on the use of force. Within this area of law, states are the dominant actors that must be responsible for measures constituting a use of force against another state. As a key aim of this thesis is to explore how cyber attacks impact on the notion of violence embodied in international law on the use of force, considering the harm caused by cyber attacks against the state entity (opposed to cyber attacks against non-state actors or other ‘multiagent systems’) was deemed most appropriate.

121 In computer science, ‘reconfiguration’ refers to the process of redefining the units of a computer system, often with the aim of providing different system functionality. See Daintith and Wright (2008).
a state, and government communications with foreign governments and regional and international organisations – various information flows continuously move in and out of this entity. The amount of global information flows also increases over time, as captured for instance by the idea of ‘Big Data.’ Similarly, more users and more devices embedded with ICTs are also constantly being connected. As such, the information storage, processing, and communication capabilities of the state also need to increase to ensure its continuing flourishing. Therefore, the informational substance of the state as a dynamic or non-static entity continuously changes over time. However, its form or pattern as an information entity persists.

The pattern or form of the state entity is evident in its systematic features. Like a ‘multiagent system’ constituted by its components, the state entity is an information system capable of interaction, it has a degree of autonomy, it is adaptable, and it has an inherent purpose towards which it gears its functions. As an information system, the state entity is situated not only in the physical world (within its territory), but also in the virtual world of

---

122 For example, the authors of a 2011 report by the McKinsey Global Institute write that:

The amount of data in our world has been exploding. Companies capture trillions of bytes of information about their customers, suppliers, and operations, and millions of networked sensors are being embedded in the physical world in devices such as mobile phones and automobiles, sensing, creating, and communicating data. Multimedia and individuals with smartphones and on social network sites will continue to fuel exponential growth. Big data—large pools of data that can be captured, communicated, aggregated, stored, and analyzed—is now part of every sector and function of the global economy. Like other essential factors of production such as hard assets and human capital, it is increasingly the case that much of modern economic activity, innovation, and growth simply couldn’t take place without data.


123 The projected number of mobile devices by 2020 is 11.6 billion which equates to 1.5 mobile devices per capita. See CISCO (2016) 'Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2015–2020', available at http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.pdf, p 3. Similarly, with the Internet of Things, more objects are becoming embedded with ICTs and capable of communicating and interacting. The idea behind this concept is described as ‘the pervasive presence around us of a variety of things or objects – such as Radio-Frequency IDentification (RFID) tags, sensors, actuators, mobile phones, etc. – which, through unique addressing schemes, are able to interact with each other and cooperate with their neighbors to reach common goals.’ Atzori et al (2010), p 2787.

124 That is, its capability to continue to care for and protect its region of the infosphere. This will be discussed in more detail below.

125 These features are based on Floridi’s description of the state as a multiagent system or ‘MAS’. He maintains that it is teleological, interactive, autonomous, and adaptable. Floridi (2014), pp 180-181. Alexander Wendt, in considering states as persons, discusses their similarity to organisms. Many of these features are similar to those attributed to states as ‘multiagent systems’ by Floridi. Wendt maintains that much like organisms: 1) states are individual as they each have a ‘distinct system with its own history’; 2) states are organised; 3) states are homeostatic as they actively resist their own degradation (which is achieved through a spatial and political closure of the boundary between the domestic and international realms, and the internal structure of the state ‘that channels the behaviour of their members toward the goal of state survival); 4) states are autonomous as ‘their behaviour is determined partly independent of their environment’; 5) however, unlike organisms they are incapable of reproduction. Wendt (2004), pp 307-309. Consequently, Wendt goes on to describe states as superorganisms, see Wendt (2004), pp 309-310.
cyberspace in which it increasingly interacts with other entities. As such, the state entity has physical and virtual properties – a presence within its territorial boundaries and a virtual presence that transcends territory. This is illustrated, for example, in the idea that the sovereignty of the state entity is considered not only to extend to the jurisdiction over the physical ICT infrastructure within its territory, but also to its conduct of ‘ICT-related activities’. Sovereignty (and the rights and obligations that flow from it) is considered to extend beyond the physical realm of international relations, to also the ‘ICT-related activities’ enabling state entities to interact and engage both in and through cyberspace. As an information system the state entity is capable of interaction and capable of cooperating and coordinating its activities with other entities. It is capable of interacting internally with the components (the sub-entities and sub-systems) that constitute its information system, as well as externally with other entities (such as other state entities, international organisations, and multinational corporations), and in some cases it constitutes a component or sub-system within these larger systems (for example, in regional or international organisations). As an information system it is autonomous in the sense that it can act independently from the other entities without being dependent on external authorisation for its actions, therefore it is not dependent on other entities for its behaviour. It is adaptable as it is capable of changing or adapting its policies and strategies depending on the information it gathers from its environment, and it can change its behaviour depending on the actions of other entities for example.

While these features reflect the state entity’s systematic nature, its form or pattern is also evident in the informational structures by which it is constituted and the protocols by which it operates. The state’s informational structures – the organisational structures of its institutions, typically seen in the structural separation of powers between legislative, executive, and judicial institutions – configure the information system’s structure as an entity. These structures that make up the information system are ‘bound together by a system of communication’, both internally within and between these structures, and externally.

127 On the features of a multiagent system in computer science, see Wooldridge (2002), p 3.
between its institutions and those of other state entities.\textsuperscript{129} The exact configuration of these structures may change among state entities (that is, the core configuration of power within the state, such as the degree or extent to which legislative, executive and judicial powers are separated). The structural configuration may also change over time (transforming states from constitutional monarchies to independent republics for example), and they can be embedded with different value systems (from secular liberal democracies to religious autocracies). However, the basic structure of these entities – their form or pattern – persists, despite continuous changes to the informational substance of these entities.\textsuperscript{130} The system of communication binding together these structures comes from the protocols according to which the communication and exchange of information occurs within this information system.

In addition to these information structures constituting the state entity as an information system, the state entity also operates according to protocols which configure it and enable it to operate as a coherent and autonomous system.\textsuperscript{131} Its internal protocols govern the interactions and information exchanges among the various sub-entities and sub-systems that it is made of. The overarching protocol according to which each information system operates generally comes from its constitution. It configures the key sub-systems within this information system (state institutions), their functions and tasks within this system, and the protocols for interaction and information exchange between these components. Various other protocols govern the interactions of these entities and humans (administrative law), the interactions between humans and corporations and the natural environment (environmental law), and the proper behaviours, interactions and information exchanges of humans and other entities within the physical and virtual environments of this information system (criminal law, civil law). Various protocols also govern the interactions of the information system as a whole with other information systems (public international law). Therefore, the information

\textsuperscript{129} Similarly, Anne-Marie Slaughter for example argues that states have become ‘disaggregated’ into networks of actors, making up what she describes as a ‘world of governments, with all the different institutions that perform the basic functions of governments—legislation, adjudication, implementation—interacting both with each other domestically and also with their foreign and supranational counterparts.’ Slaughter (2005), p 5.

\textsuperscript{130} Bynum, writing about Norbert Wiener’s ‘cybernetic account of human nature’, maintains that for Wiener ‘a person consists of a complex pattern of information embodied in matter and energy. Although the substance changes, the form must persist if the person is to flourish or even exist. Thus, a human being is an ‘information object’, a dynamic form, or pattern persisting in an ever-changing flow of matter and energy.’ Bynum (2008b), p 12 (emphasis in original).

\textsuperscript{131} In cyberspace the informational constraints of computer code – that is, the various protocols, algorithms and data structures – provide the logical (opposed to physical or legal) constraints that all entities are subject to. See Colburn and Shute (2010), p 346. Lawrence Lessig famously argued that ‘code is law’ – that is, that computer code is central to regulating behaviour in cyberspace. Lessig (2006), p 5.
structures by which the state entity as an information system is constituted, are bound together by various protocols which give the system a degree of coherence over time and delineate it as an entity separate from other information systems.

As such, the state entity is an information system – a dynamic entity constituted by various sub-systems and configured by the protocols by which it operates. With increasing amounts of information flowing in and out of it, and more and more entities becoming connected to the infosphere, the state entity becomes increasingly complex over time. The primary purpose of this entity is to care for and protect the wellbeing of its region of the infosphere. This includes the natural environment and virtual environments such as cyberspace, in which all entities increasingly coexist and interact in. The state entity has an inherent responsibility to care for and protect the entities that constitute its system – a responsibility to care for their wellbeing and protect them from entropy. By doing so and ensuring the functioning of its components and the interactions between them, it can continue to function as a system and flourish according to its nature. Caring and protecting its region of the infosphere (also ensuring its wellbeing and flourishing) includes protecting the physical territory in which it is situated, caring for the natural environment, and also caring for and protecting the virtual environment. The entities within these environments forming its region of the infosphere include everything from animals, humans, corporations, and virtual entities such as websites and databases. Therefore, the purpose of the state entity as an information system is to protect these sub-entities and sub-systems and their interactions from entropy, and care for the environments in which these entities exist.

4.2 Violence

Against this informational conceptualisation of the state entity as an information system, the harm inflicted by cyber attacks can be rethought in terms of entropy. This means that cyber

132 The notion of an entity’s ‘region of the infosphere’ is drawn from Floridi’s informational analysis of business. He considers for instance what a business is good for, maintaining that the concern is with its contribution to its ‘overall environment … [meaning] not just its physical or natural habitat, but ultimately the whole ecosystem affected by that business, by its practices and its products or, in the informational vocabulary of IE [information ethics], the region of the infosphere that is affected by that business.’ See Floridi (2013), pp 289-290.
133 Similarly, Nazli Choucri, after noting how the conventional way of thinking about national security is in terms of defending a country’s borders from military intrusions, argues that twenty-first century imperatives call for a reconsideration of this. She argues that: ‘national security must be seen as a function of four distinct but interconnected dimensions, each with its characteristic features, variables, and complexities: external security, internal security, environmental security, and cyber security.’ Choucri (2012), p 38.
attacks can be seen as a form of violence against the state as an information entity. The starting point here is the principle of ontological equality which provides that all entities have a basic right to exist and flourish. Harm to any entity is understood in terms of entropy, that is, as some form of damage, destruction, degradation, corruption or pollution of an entity, impacting on its very being and right to exist. Floridi maintains that the notion of harm is problematic, as it implies that the object of harm is a ‘sentient being with a nervous system’. Others connect harm to situations in which the interests or stakes of humans are harmed, even if those interests lie in physical objects such as buildings or plants. However, it is argued here that because all things should have value in themselves pursuant to the ontological equality principle, then any entity is capable of being ‘harmed’ even if it has no direct connection to human interests. Harm in this context is to the entity’s existence and right to flourish and, as such, to its inherent interest to exist as an information entity. Therefore, it is argued that the notion of harm does not need to be connected to purely human interests in objects or information entities. Instead, an entity is harmed when it is subject to entropy. This means that any form of damage or degradation of an entity constitutes harm because it undermines the entity’s right to exist and flourish pursuant to the ontological equality principle.

Viewing the harm inherent in any act of violence in terms of entropy however, means that on one level, with everything viewed in informational terms, all forms of violence can be seen as ‘informational violence.’ For example, intentional acts of physical harm to an entity

---

134 As Floridi writes, it is an ‘impoverishment of Being.’ Floridi (2013), p 67 (emphasis in original).
135 Floridi suggests avoiding ‘using the term ‘harm’—a zoocentric, not even biocentric, word, which implicitly leads to the interpretation of P [the patient] as a sentient being with a nervous system—in favour of ‘damage’, an onto-centric, more neutral term, with ‘annihilation’ as the level of most severe damage or highest degree of metaphysical entropy.’ Floridi (2013), p 182.
136 Joel Feinberg considers the various ways in an extended notion of harm can be used. For example, ‘[b]y smashing windows, vandals are said to harm people’s property; neglect can harm one’s garden; frost does harm to crops.’ Feinberg (1984), p 32. Similarly, according to Feinberg, machines can be harmed where their functioning is impaired and someone has an interest in its proper functioning. However, where no one has such an interest, the machine can only be described as ‘broken’ and not harmed. Feinberg (1984), p 33.
137 This is in contrast to how Feinberg describes harm. In relation to rocks for example, he writes that ‘[f]or a rock to be coherently described as broken or damaged, it must either have some special value to a human being (say, as an art object) or have some function in a larger complex that has now been impaired.’ Feinberg (1984), p 33.
138 This is not to say that any degree of entropy is always wrong and therefore, for example, that a computer virus cannot be destroyed because of its inherent right to flourish. Instead, even if any entropy in itself is considered evil, it must be considered within the wider contribution of the entity to the wellbeing of the infosphere. To this end, a normative assessment based on the four moral laws is required, and a consideration of the increases in global entropy. As discussed in chapter 2, the general approach is to consider whether the overall state of the infosphere is better, even if some entropy is caused, and hence the concern is with the global levels of entropy opposed to minor fluctuations. See Floridi (2013), pp 71-72.
resulting in damage, destruction, injury or death, that is, physical violence, can also be seen as causing entropy and amounting to informational violence. However, in order to distinguish between physical violence and forms of violence that do not result in damage or injury to, or destruction or death of an entity, the notion of informational violence will be used in a narrower sense. This allows a distinction between cyber attacks with material effects that can be likened to a form of physical violence, and those cyber attacks with non-material effects. Therefore, the notion of informational violence is used here to refer to intentional acts of non-material harm to an entity. This is to distinguish informational violence from physical violence which involves material harm to an entity. Like physical violence, informational violence too can produce entropy and harm an entity. As such, the notion of informational violence will be used to refer only to those non-material forms of harm or damage to an entity producing entropy. This is in contrast to forms of physical violence inflicting material harm to an entity. As such, the notion of informational violence captures a different ontological spectrum of violence causing entropy.

Other authors have also sought to reconsider the harm in cyber attacks. For example, Dipert suggests an ontological rethinking of the harm caused by cyber attacks. He maintains that this should involve a shift in ‘focus away from strictly injury to human beings and physical objects toward a notion of the (mal-)functioning of information systems, and the other systems (economic, communication, industrial production) that depend on them.’ He proposes the notion of cyber harm as harm inflicted through cyberspace in which ‘the functioning of a system (a person, a machine, software or an economy) is in some way impaired or degraded.’ Durante also considers the notion of violence specifically from an information ethics perspective, distinguishing between informational and physical violence. He argues that physical violence arises ‘when a disruptive activity damages, deteriorates, deletes or suppresses an informational object.’ Essentially, where the entropy that is caused physically (and not only informationally) affects the information entity so that its right to exist and not to be destroyed is infringed. He considers the separate form of ‘informational moral violence’ as violence that deprives an information entity of the capacity of being that

---

139 Dipert (2010), p 386 (emphasis in original).
140 Dipert (2010), p 397. A cyber attack is therefore intentional harm to a system, and such attacks have to be carried out by political units and need to be more than mere ‘hostile probes’ as acts of cyber espionage are. See Dipert (2010), p 397-398.
source of information that it is. He argues that moral violence in informational terms occurs when an entity is deprived of its capacity to flourish and become a specific source of information and hence become an agent. It is a form of ‘radical regardlessness’ towards an entity.

The informational reconceptualisation of violence offered here is similar to both of these accounts. Like Dipert’s cyber harm, the concern is with harm to the functioning of an entity, that is, its impairment or degradation which is captured by the notion of entropy. Also like Durante’s account of physical and informational violence, a distinction is made between the two in order to highlight the material and non-material dimensions of cyber attacks. As such, cyber attacks without material effects can be seen a form of informational violence, whereas those causing material harm constitute a form of physical violence. On a more conceptual level however, in addition to the ways in which cyber attacks actually disrupt or damage computer systems or their operation within states, they can also be seen as harming the state as an entity. Therefore, and regardless of whether they have material or non-material effects, cyber attacks can be seen as a form of violence against the state as an information entity.

Accordingly, the harm caused by cyber attacks to the state entity can be viewed in terms of entropy. Unlike the usual information flows into the state entity, cyber attacks are hostile information flows seeking to undermine or degrade the integrity the state entity, or disrupt or damage its ability to function. They do so particularly when they undermine its ability to interact, its autonomy, the protocols according to which it operates, and its ability to care for and protect the entities within its region of the infosphere. Both material and non-material cyber attacks have the ability to cause various degrees of increases in entropy, and as such, cyber attacks can be seen as forms of both physical and/or informational violence capable of causing increased entropy within state entities. In addition to the harm that they cause to computer systems or data, cyber attacks also constitute a form of violence against the state as an information entity. As such, a reconceptualisation of the state entity and the notion

144 Durante (2014), p 15. This ‘radical regardlessness’ is ‘the conceptual core or the essence of violence’ for Durante, see Durante (2014), p 10. He likens this to the deprivation of the human right to be free from torture, and argues that both physical and moral violence from an informational standpoint can be considered as ‘violence’ justifying recourse to force, see Durante (2014), pp 15-16.
of violence offers a means through which cyber attacks can be seen as capable of harming the state entity.

4.3 Law

As discussed above, the internal protocols according to which state entities operate (that is, domestic law) allow state entities to operate with a degree of coherence and autonomy. On the other hand, the external protocols of the international system govern the interactions of state entities. As demonstrated in section one of this chapter, various external protocols govern the information exchanges between state entities and restrict certain harmful information flows between them. In addition, from international human rights law to international environmental law and international economic law, a range of external protocols govern the interactions between and among state entities, corporations, human beings, and their interactions within the global infosphere. As such, law is among the protocols according to which state entities (and various other entities) operate within the international system, and it governs the interactions of these entities and the environments in which they interact.

Due to the law on the use of force, state entities within the UN Charter system are generally restricted from interactions involving material harm to other state entities. These external protocols seek to contain violence in the interactions of particular entities within the international system, and violence is conceptualised in an inherently anthropocentric and materialist way. As will be illustrated in chapter 4, while the law is capable of recognising cyber attacks with material effects as a form of violence that is prohibited, it does not adequately recognise and restrict cyber attacks with non-material effects and therefore the use of forms of informational violence in the interactions of state entities. This is despite the increasing ways in which informational violence can undermine or degrade the integrity and functioning of state entities. It is argued that the law’s inability to adequately recognise the ways in which informational violence can harm state entities is due to the ontologically constrained view of violence that is embodied in the law. As a result, informational violence is largely left outside the law’s conceptual containment of violence.

An informational reconfiguration of the law’s ontological constraints however, offers a means through which a broader spectrum of violence can be recognised by the law. Therefore, by updating the external protocols according to which the international system of
state entities operates, both informational and physical violence can be seen as threats to state entities and to international peace and security within the global infosphere. Both physical and informational violence are capable of producing increases in entropy by undermining the proper functioning of the state entity – particularly its autonomy and ability to interact, and its ability to care for and protect the entities within its region of the infosphere. Accordingly, by reconfiguring the law’s ontological constraints, also informational forms of violence can be brought into the law’s conceptual containment of violence.

Conclusion

This chapter offered an informational reconceptualisation of the state entity and the notion of violence. Doing so provides a means through which to rethink the harm that cyber attacks cause, and the state as the entity subject to violence. As such, cyber attacks can be seen as capable of harming the state as an information entity by causing increased entropy. It was argued that this reconceptualisation also enables the law to conceptually contain the informational violence that can be inflicted through cyber attacks. The first section considered various global information flows that international law has historically sought to regulate, as well as how the international community on the UN level has recognised the importance of ICTs to the functioning of modern societies. The second section explored international law’s containment of violence and demonstrated how the law traditionally regards the state as an entity and violence that is deemed to threaten the state. The third section considered the novel nature of cyber warfare and highlighted the ontological gap between kinetic and cyber warfare. Finally, section four provided an informational reconceptualisation of the state entity and the notion of violence, and argued that an informational approach offers a means to broaden the law’s conceptual containment of violence.
Chapter 4: Cyber Attacks and International Law

Introduction

This chapter argues that the threshold distinction between the non-use of force and non-intervention principles in relation to cyber attacks highlights the law’s ontologically constrained view of violence. As a result, while the law is capable of regulating cyber attacks with material effects, its capacity is limited particularly in relation to cyber attacks without material effects. This chapter is made up of two parts. Part one considers international law on the use of force and non-intervention. It demonstrates that the law conceptualises what amounts to interstate violence through the use of force doctrine, and it is argued that the law embodies an ontologically constrained view of violence. Violence in this context requires physical damage or harm (as associated with uses of armed force), whereas those measures below this threshold are considered through the non-intervention principle and effectively depicted as a form of non-violence. Part two then considers the law on the use of force and non-intervention in relation to cyber attacks. It is argued that, while the law has the capacity to regulate cyber attacks resulting in material damage to physical objects or harm to human beings, as a result of the law’s ontological constraints, it lacks the capacity to adequately deal with cyber attacks without material effects. Instead, as these cyber attacks are viewed as possible breaches of the non-intervention principle, they are depicted as forms of non-violence outside the law on the use of force and its conceptualisation of violence.

Part 1: The Use of Force and Non-Intervention

Section 1: The Use of Force

International law on the use of force and non-intervention subscribe to a particular view of the state and violence. The state is a legally constituted entity that is geographically located in physical space – an entity with a permanent population, a defined territory, a government, and the capacity to enter into relations with other states.\(^1\) The state is therefore conceptualised

---

as a territorial entity, with an aggregate of human individuals, possessing a government in control of the territory, and which has a separate existence from other entities. The law represents these entities as states, as sovereign equals within the UN Charter system that are prohibited from intervening in each other’s domestic affairs and from using force against each other’s territorial integrity or political independence. The law on the use of force and non-intervention are premised on this view of the state as a static and inherently territorial entity, and only violence of a specific type is deemed to threaten the state and international peace and security.

As highlighted in chapter 3, international law’s modern discourse on the containment of interstate violence revolves around the use of force doctrine. The formal state of war has been rendered legally obsolete and states are prohibited from using force in their international relations. Article 2(4) of the UN Charter provides that all member states of the UN:

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.

---

2 A state’s territory over which it has sovereignty under international law includes its land, the airspace above it, and, for coastal states, parts of the sea: Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v United States of America) (Merits) (1986) ICJ Reports 14 at 111 (para 212).


5 The notion of sovereign equality includes various elements including ‘that the personality of the state is respected, as well as its territorial integrity and political independence’. Goodrich et al (1969), p 37.


7 Christine Gray for instance describes Article 2(4) (and Article 51 which provides the self-defence exception to this rule) as providing ‘a new terminology and the first expression of the basic rules in their modern form.’ Gray (2000), pp 2-3.

8 In contrast to the Covenant of the League of Nations, opened for signature 28 June 1919, [1920] ATS 1 (entered into force 10 January 1920) which sought to encourage states to respect and preserve the territorial integrity and political independence of states against aggression (Article 10), and the General Treaty for the Renunciation of War as an Instrument of National Policy (Kellogg-Briand Pact), opened for signature 27 August 1928, [1929] ATS 1 (entered into force 24 July 1929) which condemned war as a means of solving disputes and renounced it as a form of national policy (Article 1), the UN Charter instead prohibits the use of force, see Charter of the United Nations, opened for signature 26 June 1945, [1945] ATS 1 (entered into force 24 October 1945), Article 2(4).

9 Charter of the United Nations, opened for signature 26 June 1945, [1945] ATS 1 (entered into force 24 October 1945), Article 2(4). Article 2(4) not only prohibits uses of force, it also prohibits any threats of such, see Legality of the Threat or Use of Nuclear Weapons (Advisory Opinion) (1996) ICJ Reports 226 at 246-247 (paras 46-48). There the ICJ noted that threats involve a ‘declared readiness’ or otherwise ‘signalled intention’ to use force, and that, for example, ‘it would be illegal for a State to threaten to secure territory from another State, or to cause it to follow or not follow certain political or economic paths’ (at 246 (para 47)). Romana Sadurska maintains that a ‘threat of force constitutes a form of coercion because it aims at the deliberate and drastic restriction or suppression by one actor of the choices of another.’ Sadurska (1988), p 241. Further, it is generally accepted that Article 2(4) only applies to uses of force between states – that is, the use of force must
This ‘cardinal principle’\textsuperscript{10} of international law has been described as ‘the very cornerstone of the human effort to promote peace in a world torn by strife.’\textsuperscript{11} Its legal force derives not only from treaty law but also from customary international law\textsuperscript{12} and it is considered to have the status of a \textit{jus cogens} norm.\textsuperscript{13}

\textsuperscript{10} \textit{Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v United States of America) (Merits)} (1986) ICJ Reports 14, at 151 (separate opinion of President Nagendra Singh).

\textsuperscript{11} \textit{Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v United States of America) (Merits)} (1986) ICJ Reports 14, at 153 (separate opinion of President Nagendra Singh). Also, the ICJ in \textit{Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v Uganda)} (2005) ICJ Reports 168 at 223 (para 148) noted that: ‘[t]he prohibition against the use of force is a cornerstone of the United Nations Charter.’ Louis Henkin has described Article 2(4) as the heart of the UN Charter framework. \textit{Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v United States of America) (Merits)} (1986) ICJ Reports 14 at 95 (para 176). Further, it maintained that ‘these norms retain a separate existence’ (at 75 (para 178)). See also Brownlie (1963), pp 267-268. See also Röling (1986), p 4; Harris (2010), pp 725-726; Shaw (2014), p 817. Therefore, under the UN Charter, the use of force is generally prohibited, unless in self-defence or authorised by the UN Security Council (Article 51 of the UN Charter permits states to use force in self-defence against an armed attack, and Chapter 7 of the UN Charter permits the Security Council to authorise the use of force to maintain or restore international peace and security).

\textsuperscript{12} The ICJ in \textit{Nicaragua v USA} rejected the argument of the United States that the treaty law prohibition on the use of force contained in Article 2(4) ‘subsume[s] and supervene[s] related principles of customary and general international law’ (at 93 (para 173)), instead finding that ‘customary international law continues to exist alongside treaty law’ and that ‘the two sources of law thus do not overlap exactly, and the rules do not have the same content.’ \textit{Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v United States of America) (Merits)} (1986) ICJ Reports 14 at 95 (para 176). Further, it maintained that ‘these norms retain a separate existence’ (at 75 (para 178)). See also Brownlie (1963), p 113; Shaw (2014), p 814.

\textsuperscript{13} Gray (2000), p 24. Crawford (2006), p 131. The ICJ in \textit{Nicaragua v USA} suggested that, the fact that states frequently refer to the prohibition on the use of force as a \textit{jus cogens} norm, confirms its validity as a customary international law norm, see \textit{Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v United States of America) (Merits)} (1986) ICJ Reports 14 at 100 (para 190). In his separate opinion, the President of the ICJ, Nagendra Singh, maintained that the application of customary international law in relation to the use of force in the judgment also ‘represents the contribution of the Court in emphasizing that the principle of non-use of force belongs to the realm of \textit{jus cogens}'. \textit{Military and Paramilitary Activities in and Against Nicaragua
The Article 2(4) prohibition on the use of force, particularly the meaning of the notion of force that it embodies, represents the central doctrine through which interstate violence is understood. As the debates about the provision’s scope reveal – from the history of its drafting to the issues raised by destructive non-kinetic weapons technologies – the generally accepted meaning is premised on a particular worldview. The law subscribes to an ontology in which the state’s territorial sovereignty is central and physical violence in particular is considered to pose a threat to states and the international order. As such, Article 2(4) is deemed to prohibit uses of armed force depicted as akin to physical violence harming the conceptual body of the state, whereas measures falling below this threshold are considered through the non-intervention principle as only affecting the personality of the state. Therefore, what follows is an examination of the notion of ‘force’ that is contained within Article 2(4), and the non-intervention principle as it is relevant in this context to those measures below the use of force threshold to illustrate how international law draws the conceptual boundaries between violence and non-violence.

The ambiguity of the notion of ‘force’ contained in Article 2(4) has given rise to various debates about its meaning.14 This central notion is not defined in the UN Charter and has been disputed.15 While acts of military aggression by states are clearly considered to constitute uses of force,16 controversy has surrounded what other types of force may fall within its ambit. Some argue that force is understood to refer only to armed force and consequently that political and economic coercion fall outside its ambit.17 This view aligns with the intention of the drafters and the UN Charter as a whole, and seeks to avoid the difficulties associated with distinguishing between permissible and impermissible forms of coercion.18 The opposite view holds that the notion of force should include political and

---

14 Though, as Christine Gray points out in the context of the drafting history of the UN Charter provisions, ‘consensus was attained only at the price of ambiguity.’ Gray (2000), p 46.
16 The UN General Assembly resolution on the Definition of Aggression provides that the use of armed force constitutes aggression (Article 1), and for example that the invasion or attack by a state’s armed forces, bombardment, blockade, or an attack on the land, sea or air forces, of marine or naval fleet of another state constitutes aggression (Article 3). Definition of Aggression (adopted by the UN General Assembly on 14 December 1974; UN Doc A/RES/29/3314).
17 For instance, Sadurska has noted that ‘[a]lthough Article 2(4) of the Charter does not specify the type of coercion it forbids, most writers assume that it refers to the physical use of armed force alone.’ Sadurska (1988), p 242 (citations omitted).
economic coercion too, as the UN Charter does not specify the prohibition to be on the use of armed force and because the use of such methods can be as threatening to the political independence of a state as military force.\textsuperscript{19} As such, both positions view that the use of traditional armed force, that is military force, is clearly included within the scope of the notion of force, but the debate is about how far beyond military force it extends.

As the UN Charter does not define ‘force’, international law specifies that the ordinary meaning of the term within the context of the object and purpose of the UN Charter should be considered.\textsuperscript{20} A dictionary definition of force defines it as ‘coercion or compulsion, especially with the use or threat of violence’.\textsuperscript{21} Coercion however, can be understood in violent and non-violent terms, resulting in a definition that is perhaps excessively broad.\textsuperscript{22} When considering the broader context and the object and purpose of the UN Charter, there is a clear desire to prevent the outbreak of war and the violence experienced in the context of the world wars. For example, among the provisions in the Preamble to the UN Charter, is the expression of a determination ‘to save succeeding generations from the scourge of war, which twice in our lifetime has brought untold sorrow to mankind’.\textsuperscript{23} One of the ways in which this is sought to be achieved is by ensuring, through ‘the acceptance of principles and the institution of methods, that armed force shall not be used, save in the common interest’.\textsuperscript{24} As such, given the overarching purpose of the UN Charter and the desire to protect future generations from the horrors of war, the notion of force should be understood within this context.\textsuperscript{25}

\textsuperscript{19} Goodrich et al (1969), pp 48-49. For instance, Oscar Schacter notes the ambiguity in the term force: ‘[i]t can be used in a wide sense to embrace all types of coercion: economic, political, and psychological as well as physical.’ Schachter (1984), p 1624.

\textsuperscript{20} The law states that terms contained in a treaty shall be interpreted so as to give them their ordinary meaning in the context of the overall object and purpose of the treaty, see Vienna Convention on the Law of Treaties, opened for signature 23 May 1969, [1974] ATS 2 (entered into force 27 January 1980), Article 31. These provisions are often referred in justification for the use of these interpretative techniques in relation to Article 2(4). For examples within the scholarship on cyber attacks and the law on the use of force and non-intervention, see Roscini (2014), p 45; Dinniss (2012), p 41, note 23; Buchan (2012), pp 215-216; Benatar (2009), p 381.

\textsuperscript{21} Stevenson (2010).

\textsuperscript{22} If force is understood as coercion that does not involve armed violence, and therefore that all forms of coercion are forbidden, then, as Tom Farer has argued in relation to the notion of a prohibition on economic or political coercion, this would even outlaw diplomacy if read literally. Farer (1985), p 406.


\textsuperscript{24} Charter of the United Nations, opened for signature 26 June 1945, [1945] ATS 1 (entered into force 24 October 1945), Preamble.

\textsuperscript{25} This is also the only reference to the notion of ‘war’ contained in the UN Charter, as the term was eliminated from legal discourse and replaced by the ‘law of force’. See Kennedy (2006), p 78. Stephen Neff similarly notes that this was ‘less an abolition of war than its reconceptualisation’. Neff (2005), p 315.
However, while Article 2(4) refers to a use of ‘force’, the Preamble refers to a qualified form of *armed* force. Looking at the UN Charter as a whole, in addition to the ‘miscellaneous’ and other related provisions about the entry into force of the UN Charter, the term ‘force’ appears five times. In addition to the Preamble and Article 2(4) contexts already mentioned, it appears in Articles 41, 44 and 46. All of these are contained in Chapter 7 of the UN Charter which deals with the authority of the UN Security Council. Essentially, Chapter 7 provides the UN Security Council with the power to ‘determine the existence of any threat to the peace, breach of the peace, or act of aggression’ and to decide on what measures to take to ‘maintain or restore international peace and security’ should such circumstances arise. Measures in this context include economic and diplomatic measures ‘not involving the use of armed force’, and, should they prove or be deemed inadequate, the UN Security Council can take action through, for instance, ‘operations by air, sea, or land forces’. Further, Article 44 provides other procedural considerations for when the UN Security Council has made its decision ‘to use force’ in this context, and Article 46 mentions the relevant committee with which the UN Security Council shall make any ‘[p]lans for the application of armed force’.

Therefore, in addition to Article 2(4), in each other instance the notion of ‘force’ appears, it clearly appears in connection with the qualified form of *armed* force or directly related to its use. Generally, according to this logic, it is understood that because everywhere else in the UN Charter the notion of force refers to armed force, then it must refer to that too in the Article 2(4) prohibition. However, others interpret it in the opposite way.

---

32 For instance, Albrecht Randelzhofer takes this approach, see Randelzhofer (2002), p 118. Dinniss adopts a similar reasoning, noting that the unqualified term of force is used only twice in the entire UN Charter and appears in its unqualified form in Article 44 but takes the qualified ‘armed force’ form in the context of Articles 41 and 46. Accordingly, she maintains that this suggests clearly ‘that the force contemplated by the unqualified term is armed.’ See Dinniss (2012), pp 41–42.
Distinguishing the instances in which armed force is referred to, from the general prohibition on the use of force in the unqualified sense, they maintain that ‘force’ in the context of Article 2(4) is not limited to armed force. Further ambiguity and confusion on what constitutes ‘force’ comes from Article 51. Here, it is stated that the UN Charter as a whole does not impair the inherent right of self-defence available to states subject to an ‘armed attack’. While an ‘armed attack’ invariably presumes a ‘use of force’, it is not so vice versa – a use of force does not necessarily always rise to the level of an ‘armed attack’ against which the use of force in self-defence is permitted. Thus there is ambiguity in interpreting the notion of ‘force’ within the context of the object and purpose of the UN Charter.

In such instances of ambiguity, or where there is need for additional support for a particular meaning that results from the application of the rules of treaty interpretation, then recourse may be had to the preparatory work of the treaty. Accordingly, the intention of the drafters of the UN Charter at the San Francisco conference contained in the preparatory work (the ‘travaux préparatoires’) is commonly referred to for clarity or additional support on how the provisions should be interpreted. Pursuant to the preparatory work of the UN Charter, the concern of the drafters with the notion of ‘force’ was military force and suggestions by the Brazilian delegation to include economic coercion were rejected. This was largely because of the experiences in the world wars and it was deemed at the time of drafting that armed force specifically was ‘simply too destructive to be considered an acceptable means of pursuing changes or advancing other policy.’ Therefore, according to the intention of the

33 The notion of ‘force’, according to Hans Kelsen, ‘is meant to include not only armed force, but any illegal action of one state which violates the legally protected interests of another’. Kelsen (2001), p 55.
36 Article 32 of the VCLT provides that where the interpretation of the terms of a treaty, even in their ordinary meaning or broader context and purpose, leaves ambiguity in their meaning, then recourse may be had to the preparatory work of the treaty. Though the VCLT generally applies only to treaties after it came into effect (1980), because it is also customary international law, the rules should apply, see Ress (2002), p 18.
38 See Randelzhofner (2002), p 118; Schmitt (1999), p 905. This is the view that is generally taken by commentators referring to the rejection of the Brazilian amendments to Article 2(4) as supportive of the interpretation that ‘force’ only refers to military force. Other commentators however, note that ‘[t]he discussions and preparatory work at San Francisco appear somewhat confused and equivocal on this point and hardly yield conclusive indication of the correctness of the commentator’s assumptions.’ McDougal and Feliciano (1994), p 124, note 8.
drafters, Article 2(4) is a prohibition on the use of armed force and not economic or political coercion.

This view is also supported by later UN General Assembly resolutions. For example, the 1970 Declaration on Friendly Relations aligns with this interpretation, referring to the prohibition on the use of force in the context of military force.\textsuperscript{40} It only refers to economic and political matters in relation to the duty not to intervene in the internal matters of a state.\textsuperscript{41} Here too there was opposition to this view as Eastern European states and most developing countries argued that force should include ‘all forms of pressure, including those of a political and economic character, which have the effect of threatening the territorial integrity or political independence of any state.’\textsuperscript{42} They argued that the notion of force should be ‘interpreted broadly so as to cover forms of coercion other than armed force.’\textsuperscript{43} This was in contrast to Western states that maintained that force only referred to armed force.\textsuperscript{44} The opposing view advocated by Eastern European states and many developing countries was rejected however, and thus political and economic coercion was to be treated under the non-intervention principle instead. Therefore, despite these debates, the 1970 Declaration on Friendly Relations was unanimously adopted and it characterises political and economic coercion as potential breaches of the non-intervention principle. As such, these forms of coercion were distinguished from uses of armed force and not considered to fall under Article

\textsuperscript{40} Declaration on Principles of International Law Concerning Friendly Relations and Co-operation among States in Accordance with the Charter of the United Nations (adopted by the UN General Assembly on 24 October 1970, UN Doc A/RES/2625(XXV)). While UN General Assembly resolutions are not a formally recognised source of law under Article 38(1) of the Statute of the International Court of Justice, opened for signature 26 June 1945, [1945] ATS 1 (entered into force 24 October 1945), they are often used as reflective the will of the international community (requiring two thirds majority to adopt them) and hence ‘persuasive evidence of legal obligation.’ Schachter (1984), p 1622. The ICJ in Nicaragua v USA, also referring to the 1970 Declaration on Friendly Relations, notes that these ‘resolutions cannot be understood as merely that of a “reiteration or elucidation” of the treaty commitment undertaken in the Charter. On the contrary, it may be understood as an acceptance of the validity of the rule or set of rules declared by the resolution themselves.’ Further, ‘that the attitude referred to expresses an opinio juris respecting such rule (or set of rules)’. Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v United States of America) (Merits) (1986) ICJ Reports 14 at 100 (para 188). The ICJ in Nicaragua v USA however, has been criticised for relying solely on UN General Assembly resolutions in defining the customary international law norm on the use of force, see Harris (2010), p 54.

\textsuperscript{41} Schmitt (1999), p 907; Declaration on Principles of International Law Concerning Friendly Relations and Co-operation among States in Accordance with the Charter of the United Nations (adopted by the UN General Assembly on 24 October 1970, UN Doc A/RES/2625(XXV)).

\textsuperscript{42} Harris (2010), p 724. For a summary of the ‘Socialist’ interpretative position on the prohibition on the use of force, see Bokor-Szegő (1986), pp 455-458.

\textsuperscript{43} Tanca (1986), p 400.

\textsuperscript{44} Tanca (1986), p 400.
Accordingly, the mainstream interpretation, supported by later UN General Assembly resolutions, is that Article 2(4) is intended to prohibit uses of armed force – specifically the violence associated with militaries using kinetic weapons in conflicts with other states.

As the UN Charter was drafted even prior to the ‘age of jets, rockets and nuclear weapons’, questions have also emerged about whether the use of non-kinetic weapons, such as chemical and biological weapons, constitute uses of armed force. Ian Brownlie famously maintained that such weapons should constitute uses of force due to the common reference to them as ‘weapons’ and, more importantly, due to their employment ‘for the destruction of life and property’. He placed importance not only on the weapon-like nature of the instruments used, but also on their destructive effects, in determining whether their use would breach Article 2(4). Similarly, the International Court of Justice (ICJ) in its advisory opinion on the Legality of the Threat or Use of Nuclear Weapons maintained that Article 2(4) does not refer to specific weapons meaning the provision applies ‘to any use of force, regardless of the weapons employed.’ Accordingly, even with the development of chemical, biological and nuclear weapons technologies, the uses of force contemplated to be prohibited by Article 2(4) clearly requires the use of weapon-like instruments capable of causing injury or death to humans, or damage or destruction of physical property.

In addition to these forms of military force, some have also discussed whether physical non-military force can constitute force for the purposes of Article 2(4). Again Brownlie remarks that:

More difficult to regard as a use of force are deliberate and forcible expulsion of population over a frontier, release of large quantities of water down a valley, and the spreading of fire through a built up area or woodland across a frontier.

---

45 Similarly, the 1987 Declaration on the Non-Use of Force (Declaration on the Enhancement of the Effectiveness of the Principle of Refraining from the Threat or Use of Force in International Relations (adopted by the UN General Assembly on 18 November 1987, UN Doc A/RES/42/22)), with reference to both Article 2(4) and the 1970 Declaration on Friendly Relations, declares the duty of states to refrain from using force in their international relations and notes that states cannot make ‘use of economic, political or any other type of measures to coerce another state’ separately from the duty to refrain from using force. See Schmitt (1999), p 907. See also Dinniss (2012), p 48.


47 Brownlie (1963), p 362.


50 Brownlie (1963), pp 362-363.
Nonetheless, he argues that, for instance in circumstances where one state controlling the upper reaches of a river releases water downstream, the ‘deliberate employment of natural forces by a state in such circumstances can probably be regarded as a use of force’. Albrecht Randelzhofer also maintains that generally non-military force would not constitute a breach of Article 2(4), and that only the non-intervention principle would apply in such circumstances. The exception to this however, is in extreme circumstances where ‘the use of physical non-military force may produce the effects of an armed attack prompting the right of self-defence’. In such cases, the use of force would not only breach Article 2(4) but also rise to the level of an armed attack warranting self-defence under Article 51. More recently it has also been suggested that non-military physical force can amount to a breach of Article 2(4) without rising to the level of an armed attack. Thus physical non-military force can in exceptional circumstances be analogous to armed military force and hence fall within the ambit of Article 2(4).

In contrast to armed force, economic coercion is not prohibited by Article 2(4). Whether it is termed ‘economic coercion’, ‘economic diplomacy’, ‘economic force’ or an economic ‘weapon’, the use of such measures is rejected as falling under the prohibition on the use of force generally due to their effects. This is despite arguments by some that the effects of economic coercion can be as severe as the use of armed force. Cassandra La-Rae Perez for instance maintains that ‘[e]conomic and trade sanctions have the potential to devastate a civilian population and to rock the economic and political stability of a developing state.’ Similarly, Jordan Paust and Albert Blaustein, referring to the 1973 Arab oil embargo, maintain that it constituted:

51 Brownlie (1963), p 376. See also Randelzhofer (2002), p 118.
57 Farer (1985), p 408.
60 Jordan Paust and Albert Blaustein refer to the 1973 Arab oil embargo as ‘the deliberate employment of an economic instrument of coercion (the oil ‘weapon’) against other states’. Paust and Blaustein (1974), p 412.
61 LaRae-Perez (2002), p 162.
coercion that threatened and might still impair not only the general wealth, well-being, and power of numerous nation-states and peoples, but also, more specifically, their national defense and security. Thus, the coercion was of such mounting intensity and efficacy that it can be authoritatively proscribed as a violation of basic Charter goals and of Article 2(4). 62

Echoing the concerns of many developing countries in the context of the 1970 Declaration on Friendly Relations, these authors argue that in some circumstances the effects of economic coercion can be contrary to the UN Charter ideals and even a violation of Article 2(4). However, as has been shown, the mainstream view remains that Article 2(4) only applies to armed force. 63 Economic coercion is therefore generally not considered a recognised form of ‘force’ to fall under the Article 2(4) prohibition.

While direct uses of armed force clearly fall within the scope of Article 2(4), the question of whether indirect uses of armed force, for instance situations in which states actively support the use of force by other actors, has also emerged. The ICJ was faced with this issue in the case of Nicaragua v USA. 64 There the US was found to have breached Article 2(4) through its involvement in, and by supporting in various ways the armed activities of the contras in Nicaragua. 65 Specifically, these included US involvement in the laying of mines in Nicaraguan ports and the destruction of various oil pipelines, oil terminals and oil storage tanks through air and sea attacks. 66 Besides a level of involvement in these attacks, the US had also provided the contras with various forms of support. The ICJ was satisfied that over the years this support had included ‘logistic support, the supply of information on the location and movement of the Sandinista troops, the use of sophisticated methods of communication, the deployment of field broadcasting networks, [and] radar coverage’. 67 These forms of support however, were not considered uses of force. Instead, the ICJ found that the ‘financial support, training, supply of weapons, intelligence and logistic support’ provided to the

63 According to Malcolm Shaw, ‘[i]t does seem that there is at least a case to be made out in support of the view that such actions are contrary to the United Nations Charter, as interpreted in numerous resolutions and declarations. But whether such action constitutes a violation of Article 2(4) is dubious.’ Shaw (2014), p 816.
66 Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v United States of America) (Merits) (1986) ICJ Reports 14 at 48 (para 81) and 50-51 (paras 85-86).
contras breached the non-intervention principle. The ICJ specifically noted that the ‘arming and training’ of the contras also constituted a use of force against Nicaragua, in contrast to ‘the mere supply of funds’ which only constituted an intervention. As such, an indirect use of armed force can also constitute a breach of Article 2(4).

Overall, the prevailing interpretation of Article 2(4) is that force here is limited to armed force. Tom Farer for example maintains that the preparatory work clearly illustrate a desire to ‘outlaw war as an instrument of state policy’ and hence that the provision is ‘concerned with violence, with military force, not with economic coercion.’ Similarly, Oscar Schachter argues that the UN Charter was designed to ‘outlaw war in its classic sense, that is, the use of military force to acquire territory or other benefits from another state.’ This is in contrast to economic and political coercion. As other commentators have noted:

while various forms of economic and political coercion may be treated as threats to the peace, as contrary to certain of the declared purposes and principles of the Organization, or as violating agreements entered into or recognized principles of international law, they are not to be regarded as coming necessarily under the prohibition of Article 2(4), which is to be understood as directed against the use of armed force.

Accordingly, the notion of ‘force’ is generally understood as ‘armed force’ and stands in contrast to other forms of coercion falling below this threshold. As alluded to earlier, these forms of coercion however, may constitute breaches of the non-intervention principle.

Therefore, Article 2(4) prohibits the use of armed force – it is concerned with a particular type of interstate violence that involves material damage or harm. It subscribes to particular ontological assumptions about the state and the forms of violence that are deemed to threaten the state and the international order. As the following section will demonstrate, international law also protects states from non-violent coercion, namely from those measures

\[68 \text{Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v United States of America) (Merits) (1986) ICJ Reports 14 at 124 (para 242).}\]
\[69 \text{Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v United States of America) (Merits) (1986) ICJ Reports 14 at 119 (para 228).}\]
\[71 \text{Farer (1985), p 410.}\]
\[72 \text{Schachter (1984), p 1624.}\]
\[73 \text{Goodrich et al (1969), p 49.}\]
below the use of force that are embodied in the modern form of the non-intervention principle protecting the ‘personality of the state’. It is argued that these distinctions demonstrate the law’s ontologically constrained view of violence, as only physical violence associated with uses of armed force is seen as a threat to the state, whereas those instances of ‘non-violence’ below this threshold are deemed outside the scope of the prohibition on the use of force.

Section 2: Non-Intervention

The mainstream meaning of the notion of ‘force’ is relatively settled as armed force, despite the aforementioned debates about how to interpret its scope. This is contrast to the less clear notion of intervention. The classic definition of intervention provided by Lassa Oppenheim is ‘forcible or dictatorial interference by a State in the affairs of another State, calculated to impose certain conduct or consequences on that other State.’ Indeed, until the twentieth century, the principle of non-intervention was only associated with the use of forceful means. For instance, in the International Law Commission’s first session in 1949, a draft provision entailing a duty on states to refrain from intervention was discussed. In this context, Hans Kelsen argued that if such a duty were interpreted in accordance with existing international law at the time, it would have meant ‘intervention by the threat or use of force.’ It was only after the world wars that the non-use of force principle took over and developed to deal specifically with military or armed force. As a result, other non-forceful but nonetheless coercive means began to be recognised as breaches of the non-intervention

---

74 See the Declaration on Principles of International Law Concerning Friendly Relations and Co-operation among States in Accordance with the Charter of the United Nations (adopted by the UN General Assembly on 24 October 1970, UN Doc A/RES/2625(XXV)).
75 The term is often used interchangeably with ‘interference,’ though ‘interference’ can be seen as a concept wider than ‘intervention’. See Jamnejad and Wood (2009), p 347, note 7; Gill (2013), p 217.
77 According to Lori Fisler Damrosch, as with most scholarly literature at the time focusing only on forms of influence involving force, ‘the prevailing viewpoint until well into the twentieth century was that the international legal concept of intervention concerned itself only with the use or threat of force against another state and not with lesser techniques.’ Damrosch (1989), p 3 (citations omitted). Tom Farer also notes how, until the decolonisation period, ‘intervention was regarded as a principle feature of the normal intercourse of international life.’ Farer (1968), p 21.
78 Article 3 of the proposed International Law Commission’s (ILC) Draft Articles on the Rights and Duties of States provided that ‘[e]very State has the duty to refrain from intervention in the internal or external affairs of any other State.’ This declaration was never adopted by the UN General Assembly, see Carbone and Schiano di Pepe (2009), paras 13-14.
79 Kelsen (1950), p 268. James Brierly also, in discussing the duty of non-intervention in this context, maintained that ‘an act of intervention was an act of dictation by one State to another state with regard to its internal or external policy backed by the use or threat of force’ emphasising that actions without an element of force, ‘however improper or unfriendly, could not be qualified as intervention.’ See ‘Summary Records and Documents of the First Session including the report of the Commission to the General Assembly’ (1949), p 90.
principle instead.\footnote{As Jamnejad and Wood maintain, ‘nowadays the international law on the use of force is not generally thought of in terms of non-intervention but as a self-standing chapter of international law.’ Jamnejad and Wood (2009), p 359.} Therefore, classically the non-intervention principle only applied to forceful interventions. While technically the principle continues to encompass both armed and non-armed forms of coercion, in the context of use of force analysis it is now generally referred to only in relation forms of coercion falling below the Article 2(4) threshold.

Unlike the non-use of force principle which exists in both treaty and customary form, the non-intervention principle is generally regarded as a principle of customary international law and hence is not manifested in a specific treaty provision alone. Nonetheless, it can be read within various treaty provisions. For instance, Article 2(1) of the UN Charter states that the UN is based on the notion of sovereign equality.\footnote{Charter of the United Nations, opened for signature 26 June 1945, [1945] ATS 1 (entered into force 24 October 1945), Article 2(1).} Sovereign equality in turn entails various elements, including the notion ‘that the personality of the state is respected, as well as its territorial integrity and political independence’.\footnote{See Goodrich et al (1969), p 37.} The principle is also alluded to in Article 2(7) of the UN Charter which provides that the UN cannot ‘intervene in matters which are essentially within the domestic jurisdiction of any state’.\footnote{Charter of the United Nations, opened for signature 26 June 1945, [1945] ATS 1 (entered into force 24 October 1945), Article 2(7).} Similarly, the principle can be seen in various regional treaties.\footnote{Jamnejad and Wood (2009), p 364.}

For the content of the non-intervention principle, two key declarations by the UN General Assembly stand out. The 1965 Declaration on the Inadmissibility of Intervention\footnote{Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of their Independence and Sovereignty (adopted by the UN General Assembly on 21 December 1965, UN Doc A/RES/20/2131(XX)).} condemns all forms of interference with the personality of a state\footnote{Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of their Independence and Sovereignty (adopted by the UN General Assembly on 21 December 1965, UN Doc A/RES/20/2131(XX)), p 12.} and the similarly worded 1970 Declaration on Friendly Relations\footnote{Declaration on Principles of International Law Concerning Friendly Relations and Co-operation among States in Accordance with the Charter of the United Nations (adopted by the UN General Assembly on 24 October 1970, UN Doc A/RES/2625(XXV)).} states that such actions are in violation of international law:
No State or group of States has the right to intervene, directly or indirectly, for any reason whatever, in the internal or external affairs of any other State. Consequently, armed intervention and all other forms of interference or attempted threats against the personality of the State or against its political, economic and cultural elements, are in violation of international law.\(^\text{88}\)

While the 1970 Declaration on Friendly Relations is not a treaty and does not have binding force as such, it is regarded as an authoritative statement of the principle. This is because it was adopted unanimously by the UN General Assembly, and also because it was heavily relied upon by the ICJ in *Nicaragua v USA*. The ICJ relied on it both as support for the existence of the principle in customary international law, as well as for the content of the principle.\(^\text{89}\)

The ICJ in *Nicaragua v USA* discussed the principle of non-intervention stating that:

A prohibited intervention must accordingly be one bearing on matters in which each State is permitted, by the principle of State sovereignty, to decide freely. One of these is the choice of a political, economic, social and cultural system, and the formulation of foreign policy. Intervention is wrongful when it uses methods of coercion in regard to such choices, which must remain free ones. The element of coercion, which defines, and indeed forms the very essence of, prohibited intervention, is particularly obvious in the case of an intervention which uses force.\(^\text{90}\)

This principle is regarded as containing two elements: first, there must be an intervention, and second, it must impact on those choices which should be freely made by states.\(^\text{91}\) Unlike uses of force which require a degree of physicality, the non-intervention principle applies to those forms of coercion that only affect the ‘personality of the state’ by impacting on the matters

\(^{88}\) Declaration on Principles of International Law Concerning Friendly Relations and Co-operation among States in Accordance with the Charter of the United Nations (adopted by the UN General Assembly on 24 October 1970, UN Doc A/RES/2625(XXV)), p 123 (emphasis added).

\(^{89}\) *Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v United States of America) (Merits)* (1986) ICJ Reports 14 at 101, 106 (paras 191, 202). The ICJ in *Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v Uganda)* (2005) ICJ Reports 168 at 226-227 (para 162) referred to the provisions of the 1970 Declaration on Friendly Relations as ‘declaratory of customary international law.’ While the 1981 Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs of States (adopted by the UN General Assembly on 9 December 1981, UN Doc A/RES/36/103) also refers to the non-intervention principle, it is commonly criticised for its broad scope and for the number of states voting against it (and number of abstentions), see Jamnejad and Wood (2009), p 355.

\(^{90}\) *Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v United States of America) (Merits)* (1986) ICJ Reports 14 at 108 (para 205).

\(^{91}\) Jamnejad and Wood (2009), p 347.
that states should be able to decide freely.\textsuperscript{92} For example, in \textit{Nicaragua v USA}, as noted above, the US actions amounted to a use of force because it was involved in various attacks and in the ‘arming and training’ of the contras. In contrast, the other forms of support that the US provided, which included logistical, informational and communicational support, only amounted to an intervention.\textsuperscript{93} The support itself constituted the ‘intervention’ (first element), whereas the coerciveness (second element) was satisfied as the ICJ found that the US did this with the intention ‘to coerce the Government of Nicaragua in respect of matters in which each State is permitted, by the principle of State sovereignty, to decide freely’\textsuperscript{94}.

The ICJ in \textit{Nicaragua v USA} also discussed the relationship of the non-intervention principle to the non-use of force. Essentially the non-intervention principle is broader than the non-use of force principle but generally only referred to when coercive activities do not reach the level of a prohibited use of force. For instance, when discussing actions that would amount to a prohibited intervention, the ICJ noted that actions amounting to a ‘use of force’ would be ‘wrongful in the light of both the principle of non-use of force, and that of non-intervention.’\textsuperscript{95} With respect to the ‘use of force’, the ICJ distinguished between forms of force depending on their gravity. It distinguished ‘the most grave forms of use of force (those constituting an armed attack) from other less grave forms.’\textsuperscript{96} Here it also noted that certain conduct may amount to a breach of ‘the principle of the non-use of force and an intervention in the internal affairs of a State, that is, a form of conduct which is certainly wrongful, but is of lesser gravity than an armed attack.’\textsuperscript{97} Therefore, according to the ICJ in \textit{Nicaragua vs USA}, there are three different types of coercion which can be distinguished by their gravity. Coercion however remains the operative element, ‘the very essence’ of prohibited

\begin{itemize}
\item \textsuperscript{92} According to Cassese, it ‘prohibits States from encroaching upon the internal affairs of other States. Thus, for instance, a State is not allowed to bring pressure to bear on \textit{specific national bodies} of other countries’. Cassese (2005), p 53 (emphasis in original).
\item \textsuperscript{93} \textit{Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v United States of America) (Merits)} (1986) ICJ Reports 14 at 61 (para 106).
\item \textsuperscript{94} \textit{Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v United States of America) (Merits)} (1986) ICJ Reports 14 at 124 (para 241).
\item \textsuperscript{95} \textit{Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v United States of America) (Merits)} (1986) ICJ Reports 14 at 108 (para 205). This was affirmed by the ICJ in \textit{Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v Uganda)} (2005) ICJ Reports 168 at 227 (para 164).
\item \textsuperscript{96} \textit{Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v United States of America) (Merits)} (1986) ICJ Reports 14 at 101 (para 191).
\item \textsuperscript{97} \textit{Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v United States of America) (Merits)} (1986) ICJ Reports 14 at 127 (para 247).
\end{itemize}
interventions and ‘obvious’ in uses of force. These are: 1) forms of coercion affecting matters that states are free to decide (prohibited interventions); 2) coercive armed force (prohibited uses of force); and 3) coercive armed force rising to the level of an armed attack (against which the use of force is permitted in self-defence).

Coercion is thus a key element separating those acts by states that may be considered in breach of the non-intervention principle from legitimate pressure. Maziar Jamnejad and Michael Wood for example stress that:

The requirement of coercion is a crucial limit in the principle of non-intervention. Without it, any act which had an effect on another state could fall within the prohibition. The requirement of coerciveness not only removes minor international friction from the scope of the principle, but means that it only applies to those acts that to some degree ‘subordinate the sovereign will’ of another state.

Others have also described the non-intervention principle as ‘the doctrinal mechanism to express the outer limits of permissible influence that one state may properly exert upon another’ and ‘the frontier between diplomatic pressure which is tolerable to the pressured and various degrees of coercion which are not.’

Therefore, in exploring the meaning of force within Article 2(4), and the non-intervention principle as it is relevant to the threshold distinction between these principles, this part has examined the way in which the law conceptualises interstate violence. Violence is regarded as something inherently physical – as associated with uses of armed force – opposed to those non-forceful measures that fall within the ambit of the non-intervention principle alone and are effectively depicted as a form of non-violence. It is therefore argued that the law reflects an ontologically constrained view of violence. The state is viewed as a static territorial entity and violence requires physical damage or harm as associated with uses

---

98 Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v United States of America) (Merits) (1986) ICJ Reports 14 at 108 (para 205). David Harris has also noted that ‘[a]n armed attack upon another State annexing its territory is the ultimate form of intervention.’ Harris (2010), p 743.
99 The ICJ also goes on to list these as ‘the choice of a political, economic, social and cultural system, and the formulation of foreign policy.’ Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v United States of America) (Merits) (1986) ICJ Reports 14 at 108 (para 205).
101 Jamnejad and Wood (2009), p 381.
of armed force. Particularly where there is neither harm to human beings nor damage to physical property, the law is effectively incapable of recognising this as a form of violence. Instead, it is depicted as below the use of force threshold and within the scope of the non-intervention principle alone. As a result of this, as will be demonstrated in the following part, while the law is capable of regulating cyber attacks that result in material damage or harm, it lacks the capacity to sufficiently deal with cyber attacks with non-material effects.

**Part 2: Cyber Attacks, the Use of Force, and Non-Intervention**

This part considers existing literature on cyber attacks and the use of force and non-intervention. It is argued that the law’s ontologically constrained view of violence is evident in the dominant approaches to the application of these doctrines to cyber attacks. As the law is centrally concerned with protecting the state entity from the physical violence associated with uses of armed force, it has the capacity to regulate cyber attacks with material effects. This is evident in the fact that cyber attacks with material effects, such as damage or destruction of property or injury or death to human beings, are considered the easy cases for the use of force analysis. The more complex instances of cyber attacks however, affecting the functionality of ICTs or otherwise disruptive attacks without material effects, are generally not considered as uses of force because they do not fit into existing conceptualisations of violence. These cyber attacks below the use of force threshold are considered as potential breaches of the non-intervention principle instead, and effectively depicted as forms of non-violence. Therefore, it is argued that the law lacks the capacity to recognise non-material or primarily disruptive cyber attacks as a form of violence prohibited by the law on the use of force. It is argued that this is due to the ontologically constrained view of violence embodied in the law, meaning non-material cyber attacks escape the conceptual containment of violence achieved by these doctrines.

**Section 1: Cyber Attacks and the Use of Force**

Given the increased dependence of states on ICTs and cyberspace that was demonstrated in chapter 3, states have become vulnerable to cyber attacks and also acquired the capability to engage in cyber warfare. Technology has thus made it possible for states to engage in new ways both in and through cyberspace, raising questions about the application of international law in this context. This is because, according to the classic *Lotus* principle, international law
permits what it does not expressly prohibit. In fact, some early views held that cyberspace should be a zone entirely outside the control of states. In contrast however, in 2012 the United States’ Department of State’s legal advisor, Harold Koh, expressly declared the US position and what is now the generally accepted position, that international law applies in cyberspace and that it is not a law free zone. As a zone within the realm of law, international lawyers and scholars have also dealt with the question of how the law should be applied in the cyber context, and the most prevalent ways of doing so have been through analogy or the extension of existing law. A range of areas of law have been considered, including the law regulating the use and proliferation of nuclear weapons, international telecommunications law, aviation law, outer-space law, the law governing Antarctica, and the law of the sea. Through analogy or extension, these laws are used or offered as ways of conceptualising how the law already applies or how it could apply to state activities in cyberspace, including to the use of cyber attacks. Given the general prohibition on the use of force in international law, the question of whether and when a cyber attack constitutes a use of force has been a central focus. With no hard law on the use of cyber attacks specifically, an important soft law instrument comes from the Tallinn Manual on the International Law Applicable to Cyber Warfare (Tallinn Manual). This study was published in 2013 and it was authored by an International Group of Experts (Group of

106 Koh (2012). Scott Shackelford for instance notes how cyberspace ‘is far from the untamed digital Wild West that it is at times made out to be.’ Shackelford (2014), p 311.
107 Shackelford for example highlights how cyber attacks can in worst-case scenarios cause indiscriminate destruction similar to nuclear attacks, therefore existing law surrounding the use of nuclear weapons should apply to them by analogy. Shackelford (2009), pp 218-219.
109 Hathaway et al consider various international aviation laws that co-ordinate and regulate the safe and proper use of aircrafts and aviation. By extension, cyber attacks that interfere with civilian aircrafts or endanger their safe flight would violate these rules. See Hathaway et al (2012), pp 868-870.
111 Shackelford considers whether cyberspace could be treated like Antarctica as an area of commons in which military activity is banned. Shackelford (2009), pp 222-223.
113 See also Shackelford (2014), pp 267-268. However, see for example Duncan Hollis who suggests that ‘perhaps the conventional wisdom on the viability of IO [information operations] law by analogy is simply wrong.’ Hollis (2007), p 1053.
114 Harris describes soft law as consisting of ‘written instruments that spell out rules of conduct that are not intended to be legally binding, so that they are not subject to the law of treaties and do not generate the opinio juris required for them to be state practice contributing to custom.’ Harris (2010), p 57 (citations omitted).
Experts) led by Michael Schmitt. It considers both the *jus ad bellum* and *jus in bello* in relation to cyber warfare. On the central questions relating to the law on the use of force – whether the use of cyber attacks is prohibited, if so, when the use of cyber attacks is prohibited – the Tallinn Manual provides that:

**Rule 10:** 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.\(^\text{117}\)

Accordingly, the Group of Experts took the view that cyber attacks can constitute a use of force and be considered unlawful under existing law on the use of force. As to the question of when a cyber attack constitutes a use of force, the Group of Experts provided that:

**Rule 11:** 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.\(^\text{118}\)

As such, the Tallinn Manual seeks to answer what are among the key questions for international law in relation to cyber attacks, namely whether the law on the use of force extends to cyber attacks, and if so, what sort of harm amounts to ‘force’ that is prohibited by the law.\(^\text{119}\) Essentially, the answer it provides is that the law on the use of force applies to cyber attacks, and a cyber attack constitutes a use of force when it is comparable ‘in scale and effects’ to a non-cyber use of force.\(^\text{120}\) While this is clear, according to the Tallinn Manual, in instances where people are killed or physical objects are destroyed,\(^\text{121}\) it is less clear where no injury to human beings or damage to physical objects occurs.\(^\text{122}\)

---


\(^{118}\) Rule 11, Schmitt (2013b), p 45.


\(^{120}\) However, a key limitation of the Tallinn Manual, something Schmitt has expressly acknowledged, is that the study was about the application of *existing* law to cyber warfare, and not about what the law ought to be or how it may develop. See Schmitt (2014), p 270.

\(^{121}\) On when acts below the threshold of an ‘armed attack’ nonetheless constitute a use of force, the Group of Experts maintained that ‘[a]cts that injure or kill persons or damage or destroy objects are unambiguously uses of force.’ See Commentary to Rule 11, Schmitt (2013b), p 48. This is similar to Schmitt’s position in his seminal article published in 1999, where he maintained that a cyber attack constitutes armed force as prohibited by Article 2(4) ‘if the attack is intended to directly cause physical damage to tangible objects or injury to human beings.’ Schmitt (1999), p 934.

In the broader international legal scholarship on whether cyber attacks amount to a use of force or not, three different approaches are evident. The ‘instrument approach’ is in essence concerned with the nature of the instrument used – where a ‘weapon’ or similar instrument is used to inflict the force then it may amount to a use of armed force.\(^{123}\) The ‘target approach’ in turn focuses on the target of the cyber attack – where this is important infrastructure for instance, it should be considered a use of force.\(^{124}\) Finally, the ‘effects approach’ is concerned with the effects of cyber attacks and whether they are comparable to those of conventional military attacks.\(^{125}\) Few adopt a single approach by itself, and these are more so used to distinguish between various considerations in assessing whether a cyber attack amounts to a use of force. Marco Roscini for instance combines the ‘instrument approach’ and ‘effects approach,’ suggesting that whether a cyber attack amounts to a use of force or not must be determined by the weapons (instruments) used however, ‘weapons’ are defined by the harmful effects of the instrument in question.\(^{126}\) Accordingly, for Roscini it is the ‘instrument used that defines armed force, but the instrument is identified by its (violent) consequences.’\(^{127}\) Similarly, William Boothby adopts the position that a cyber weapon is defined by its violent consequences – where a means of cyber attack is ‘designed, intended or used, in order to have violent consequences, that is, to cause death or injury to persons or damage or destruction of objects.’\(^{128}\) As these combined approaches already highlight, the effects of a cyber attack are particularly important in the analysis of cyber attacks and the use of force.

The ‘instrument approach’ considers the nature of the instrument being used and whether it constitutes a weapon and therefore a use of ‘armed’ force. This was also the approach traditionally used in distinguishing armed force from economic and political coercion.\(^{129}\) As Schmitt notes, this determination generally

\[\text{(126 Roscini (2014), pp 49-50.}\]
\[\text{(127 Roscini (2014), p 50.}\]
\[\text{(128 Boothby (2013), p 389.}\]
\[\text{(129 Schmitt (1999), p 909; Roscini (2014), pp 46-47.}\]
instruments might rise to the level of intervention, but they do not engage the normatively more flagrant act of using force.\textsuperscript{130}

The problem with adopting a purely ‘instrument approach’ in relation to cyber attacks however, comes from their non-physical nature and non-weapon-like qualities.\textsuperscript{131} The essential question is, according to Heather Harrison Dinniss, ‘whether a bitstream of malicious code is sufficiently militaristic or weapon-like to meet the required definition of ‘armed’ force.’\textsuperscript{132} Unlike conventional weapons, cyber attacks are at their core ‘simply written instructions that are translated into the 0s and 1s of binary code, the language of machines.’\textsuperscript{133} As such, cyber weapons are at odds with the conventional understanding of what constitutes a weapon, particularly as they lack the physicality associated with weapons.

Further, weapons generally generate destructive effects through kinetic force, and while chemical and biological weapons for instance do so through non-kinetic force, they are nonetheless widely recognised and regarded as weapons.\textsuperscript{134} Cyber weapons in contrast can reside, for example, on small USB drives and can be released by the mere stroke of a key.\textsuperscript{135} However, focusing purely on the instrument used is problematic in the cyber context given the non-weapon-like nature of digital code and that, from this perspective, even potentially destructive cyber attacks may be excluded from constituting a use of ‘armed force.’\textsuperscript{136}

Similarly, as discussed above, the approach taken in relation to chemical and biological weapons was concerned with both their weapon-like nature and their destructive effects. Indeed, the nature of the weapon technology is generally not an issue as it depends on how it is used. A laser beam for instance can be used for beneficent medical purposes or destructive and lethal purposes.\textsuperscript{137} As Daniel Silver argues: ‘when we assign one of those technologies to the “armed force” category, it is not because of its inherent lethality but because of the potential destructiveness of the way it is being used or the purpose for which it is deployed.’\textsuperscript{138} Therefore, cyber weapons lack the physicality and weapon-like nature of what are traditionally understood as weapons, despite that they can potentially cause destruction.

\textsuperscript{130}Schmitt (1999), p 909.
\textsuperscript{131}Hollis (2007), p 1041.
\textsuperscript{132}Dinniss (2012), p 68.
\textsuperscript{133}Nguyen (2013), p 1127.
\textsuperscript{134}Boothby (2013), pp 388-389. See also Brownlie (1963), p 362.
\textsuperscript{135}Boothby (2013), p 389.
\textsuperscript{136}Roscini (2014), p 47.
\textsuperscript{137}Silver (2002), p 88.
\textsuperscript{138}Silver (2002), p 88.
As such, considering the question of whether cyber attacks can constitute armed force by focusing purely on the ‘instrument approach’ is problematic.

The ‘target approach’ is primarily concerned with the target of the cyber attack in determining whether or not it would amount to a use of force. The key factor here is the value of the computer system or network to a state’s critical national interests.\(^{139}\) Roscini uses the example of a cyber attack against critical infrastructure:

A week-long cyber attack that shuts down the national grid, and thus leaves millions of people without electricity, cripples the financial market and the transport system, and prevents government communications is likely to be treated as a use of force, whether or not physical damage ensues.\(^{140}\)

In contrast, he maintains that a similar attack on a (non-critical) network such as that of a university would not amount to a use of force.\(^{141}\) Similarly, Eric Talbot Jensen for instance has suggested that attacks on critical infrastructure from *any source* (including cyber attacks) would amount to a use of force.\(^{142}\) As Duncan Hollis however notes, cyber attacks can range from merely disruptive to highly destructive, and if the focus is simply on the ‘critical’ nature of the target, then very minor attacks can potentially be considered uses of force.\(^{143}\)

Consequently, while the target of a cyber attack is an important consideration, reliance on the target approach alone is also problematic.

From the ‘effects approach,’ a cyber attack is assessed based on its effects. This approach has attracted most support, and its focus is on the evaluation of whether the effects of a cyber attack are akin to a use of armed force. For instance, the Tallinn Manual’s Group of Experts, while considering several criteria, highlighted the severity of an attack as the ‘most significant’ criterion to be considered.\(^{144}\) While an early example of this view considered that cyber attacks causing *any* destructive effect against information for instance, would amount to an unlawful use of force, more recent views only consider those attacks

\(^{139}\) Sharp (1999), pp 129-130.
\(^{140}\) Roscini (2014), p 62.
\(^{141}\) Roscini (2014), p 63. Roscini thus argues that ‘only cyber attacks that go beyond mere inconvenience and *significantly* disrupt the functioning of *critical* infrastructure that can potentially fall under the scope of Article 2(4).’ Roscini (2014), p 62 (emphasis in original).
\(^{142}\) Jensen (2002), pp 208-209.
\(^{143}\) Hollis (2007), p 1042.
\(^{144}\) Commentary to Rule 11, Schmitt (2013b), p 48. They also noted that the severity of an attack is influenced by its scope, duration and intensity.
with tangible effects as qualifying.\textsuperscript{145} As such, according to the prevailing view, cyber attacks that have material effects such as damage to physical objects or injury to human beings constitute the ‘easy cases’ that most clearly amount to a use of force. Reliant on Brownlie’s effects based approach focusing particularly on whether there was any ‘destruction of life or property’,\textsuperscript{146} Barkham for instance argues that cyber attacks that cause instantaneous destruction akin to that caused by conventional weapons are ‘relatively easy’ to regard as constituting uses of force.\textsuperscript{147} Schmitt also notes that the narrow category of cyber attacks ‘specifically intended to directly cause physical damage to tangible property or injury or death to human beings’ are ‘easily dealt with.’\textsuperscript{148} For Dinniss ‘it appears to be clear’ that a cyber attack will constitute a use of force where it ‘results in a physical consequence, namely destruction of physical property, injury or loss of lives.’\textsuperscript{149} According to Herbert Lin too, ‘the ambiguities are fewest when cyber attacks cause physical damage to property and loss of life in ways that are comparable to kinetic attacks and traditional war’.\textsuperscript{150} Roscini in turn maintains that the position is ‘virtually uncontested’\textsuperscript{151} that if a cyber attack causes physical damage to property or injury to persons then it would amount to a use of force.\textsuperscript{152} Similarly, Katharina Ziolkowski, noting the ‘nearly uniform opinion among scholars’, also takes the view that a cyber attack amounts to a use of force ‘if it results in death, physical injury or the destruction of property.’\textsuperscript{153} Silver also argues that a cyber attack will most likely constitute a use of force where ‘its direct and foreseeable effects are physical injury or property damage.’\textsuperscript{154} Joyner and Lotrionte in turn find it ‘persuasive’ that cyber attacks which ‘directly and intentionally result in non-combatant deaths and destruction’ constitute uses of force.\textsuperscript{155} Yoram Dinstein too maintains that the crux of whether a cyber attack amounts to a use of force is not the means used but its ‘violent consequences’.\textsuperscript{156} Finally, the Group of Experts also maintained that generally ‘[a]cts that injure or kill persons or damage or destroy objects are unambiguously uses of force’\textsuperscript{157} and where cyber attacks have similar consequences, they

\textsuperscript{145} Sharp (1999), p 133.
\textsuperscript{146} Barkham (2001), p 72 citing Brownlie (1963), pp 362-363.
\textsuperscript{147} Barkham (2001), p 80.
\textsuperscript{148} Schmitt (1999), p 913. Jack Goldsmith has taken a similar approach, see Goldsmith (2013), p 133. See also Hoisington (2009), p 447.
\textsuperscript{149} Dinniss (2012), p 74.
\textsuperscript{150} Lin (2010), p 73.
\textsuperscript{151} Roscini (2014), p 53.
\textsuperscript{152} Roscini (2014), p 53.
\textsuperscript{153} Ziolkowski (2010), p 70.
\textsuperscript{154} Silver (2002), p 85.
\textsuperscript{155} Joyner and Lotrionte (2001), p 850.
\textsuperscript{156} Dinstein (2002), p 103.
\textsuperscript{157} Commentary to Rule 11, Schmitt (2013b), p 48.
are ‘highly likely’ to constitute uses of force. Therefore, despite their non-physical nature as weapons, a cyber attack can also constitute a use of force under Article 2(4) especially if it has material effects.

In addition to the rules provided by the Tallinn Manual that were outlined above, the Group of Experts also considered eight criteria in the commentary to the Tallinn Manual to aid in the determination of when a cyber attack constitutes a use of force. These criteria were based on six criteria that Schmitt first suggested in the late 1990s and they have been widely cited since. Therefore, the following eight criteria were regarded by the Group of Experts as a non-exhaustive list of factors to consider in distinguishing armed force from other forms of coercion, and specifically in determining the circumstances in which a cyber attack would amount to a use of force in breach of Article 2(4).

1) Severity: compared to economic and political coercion, coercion through the use of armed force ‘threaten[s] physical injury or destruction of property to a much greater degree’. Cyber attacks causing physical harm to people or destruction of property will thus generally amount to a use of force, whereas those causing purely inconvenience or irritation will never qualify.

2) Immediacy: the negative effects of armed force are more immediately visible than those from other forms of coercion. Where the effects are immediate, there are fewer opportunities to peacefully resolve the situation or mitigate its harmful effects.

3) Directness: in terms of the chain of causation, the consequences of armed force are more directly linked to the act itself, whereas the effects of other forms of coercion are indirect and dependent on other contributing factors. Hence cyber attacks in

---

159 Schmitt (1999), pp 914-915.
165 Commentary to Rule 11, Schmitt (2013b), p 49.
166 Schmitt (1999), p 914.
which the cause and effect are clearly linked are most likely to constitute uses of force.\textsuperscript{167}

4) Invasiveness: armed force usually intrudes through the borders of a target state, whereas acts of economic coercion usually occur outside those borders.\textsuperscript{168} Cyber attacks will be most invasive when they penetrate the most secure systems, opposed to mere exploitation of vulnerabilities in more openly accessible systems.\textsuperscript{169} Also, cyber attacks concentrated into a particular state will increase their perceived invasiveness.\textsuperscript{170}

5) Measurability: the negative consequences of armed force are usually easier to measure and quantify, compared to other forms of coercion.\textsuperscript{171} While the consequences of cyber attacks are generally less apparent, those attacks that result in more specifically measurable effects are more likely to constitute a use of force.\textsuperscript{172}

6) Military character: generally cyber attacks that occur in close connection to uses of military force will increase the likelihood of them constituting uses of force.\textsuperscript{173}

7) State involvement: where there is a high degree of clear state involvement in a cyber attack, it is more likely other states will regard it as a use of force.\textsuperscript{174}

8) Presumptive legitimacy: under both domestic and international law, it is generally presumed that the application of violence is illegitimate (unless authorised, for instance, in self-defence). In contrast, economic and political coercion are generally regarded as permissible.\textsuperscript{175} Similarly, propaganda and espionage are not expressly prohibited under international law and are generally permitted. Accordingly, cyber attacks that only amount to economic coercion or espionage for instance are less likely to constitute uses of force.\textsuperscript{176}

As Schmitt noted when he originally coined these criteria, given the new forms of coercion made possible by cyber attack technologies, these criteria are useful in rethinking the boundaries of the use of force ‘box’ so that it can be expanded to fill in gaps in the law that

\begin{itemize}
\item \textsuperscript{167} Commentary to Rule 11, Schmitt (2013b), p 49.
\item \textsuperscript{168} Schmitt (1999), p 914.
\item \textsuperscript{169} Commentary to Rule 11, Schmitt (2013b), p 49.
\item \textsuperscript{170} Commentary to Rule 11, Schmitt (2013b), p 49.
\item \textsuperscript{171} Schmitt (1999), p 915.
\item \textsuperscript{172} Commentary to Rule 11, Schmitt (2013b), p 50.
\item \textsuperscript{173} Commentary to Rule 11, Schmitt (2013b), pp 50-51.
\item \textsuperscript{174} Commentary to Rule 11, Schmitt (2013b), p 51.
\item \textsuperscript{175} Schmitt (1999), p 915.
\item \textsuperscript{176} Commentary to Rule 11, Schmitt (2013b), p 51.
\end{itemize}
have been revealed by cyber attacks.\textsuperscript{177} Questions of responsibility and the problematic ‘presumptive legitimacy’ aside,\textsuperscript{178} essentially the threshold question of cyber attacks amounting to armed coercion is concerned with invasive attacks that directly cause, immediately visible, severe and quantifiable effects such as death or destruction. Therefore, aligning with the dominant position in the scholarly literature on cyber attacks and the use of force, essentially where cyber attacks have destructive physical effects causing injury to humans or damage to property, they will constitute a use of force as prohibited by Article 2(4). These are considered the easy cases.

The more complex cases come from those cyber attacks that do not directly cause visible physical harm, such as injury to humans or damage to property. Usually it is the use of lower intensity cyber attacks that is considered to exploit the traditional distinctions between armed force and other forms of coercion.\textsuperscript{179} Indeed, according to Dinniss, the non-physical nature of the effects of a cyber attack is the characteristic causing ‘the most uncertainty in applying the legal requirements of force and the laws of war.’\textsuperscript{180} She notes that in some instances there is no tangible target as the target of the attack only exists as information.\textsuperscript{181} Such attacks can have varying effects and are problematic especially ‘where the effect of the attack is not to destroy the information, but to degrade the information target to the extent that it cannot be relied upon.’\textsuperscript{182} Hence also depending on the target, the effects may or may not manifest in physically harmful or destructive effects.\textsuperscript{183} Therefore, cyber attacks do not even necessarily result in the destruction of intangible property such as information, but sometimes merely degrade its integrity. Barkham also notes this, namely that those cyber attacks that only undermine the integrity of data, as opposed to actually destroying it, are problematic. He uses the examples of DDoS attacks and industrial espionage which can ‘rob the property of its value without causing any actual physical damage.’\textsuperscript{184} However, he maintains that such attacks would not be considered uses of force as there is no weapon

\begin{itemize}
\item \textsuperscript{177} Schmitt (1999), p 915. He also notes that ‘[u]ntil the advent of information operations, most coercion could be handily categorized into one of several boxes, for few coercive options existed that could not be typed as political, economic, or armed in nature.’ Schmitt (1999), p 908.
\item \textsuperscript{178} The sixth criterion has been criticised by Jason Barkham, who notes that if the question is whether a cyber attack constitutes an (illegitimate) use of force or a (legitimate) form of coercion, one of the criteria for making that assessment of legitimacy cannot be whether the act is considered legitimate or not. Barkham (2001), pp 85-86. For a critical discussion of these criteria in general, see Ziolkowski (2012a), pp 301-308.
\item \textsuperscript{179} Barkham (2001), p 58.
\item \textsuperscript{180} Dinniss (2012), p 72.
\item \textsuperscript{181} Dinniss (2012), pp 67-68.
\item \textsuperscript{182} Dinniss (2012), p 68.
\item \textsuperscript{183} Dinniss (2012), p 68.
\item \textsuperscript{184} Barkham (2001), p 89.
\end{itemize}
involved nor property destroyed.\textsuperscript{185} He highlights that in these instances ‘[t]he target might be whole afterwards, but the parties would be harmed as a result.’\textsuperscript{186} This is particularly the case in relation to cyber attacks of the lowest intensity:

the lowest level of IW [information warfare] attacks further complicates the use of force analysis because such attacks neither cause damage nor substantially impair the target network. When one state probes the servers of another, there is neither harm to life or property nor any physical impact whatsoever.\textsuperscript{187}

These problems are identified by other authors too. Georg Kerschischnig for instance notes the problems associated with the need for physical damage or destruction under the use of force doctrine. He maintains that ‘[t]he strict limitation to physical damage clearly does not reflect the realities of cyberspace.’\textsuperscript{188} While physical damage is a possible result of a cyber attack, the norm tends to be ‘intangible damage caused to the software and data.’\textsuperscript{189} Scott Shackelford maintains that difficulties arise in relation to ‘pure information’ attacks involving electronic means to access or alter information without ‘damag[ing] any physical components in the traditional sense.’\textsuperscript{190} Similarly, Boothby questions whether ‘damage to data within a computer system that does not affect the facility or service that the targeted computer system provides constitutes damage’.\textsuperscript{191} Adopting the position taken by the Group of Experts, he maintains that the data resident on a computer system can only be properly regarded as an object of an attack under limited circumstances. The attack must impact on the functioning of a computer systems or network to the degree that repairs are needed for it to be able to operate again.\textsuperscript{192} Roscini also notes a similar problem in relation to intangible property, questioning:

Whether data as such can be equated to physical property for the purposes of Article 2(4), so that their deletion, alteration or corruption qualifies as a use of force even without physical damage or incapacitation of infrastructure, is a question that it is very difficult to answer.\textsuperscript{193}

\begin{footnotesize}
\begin{itemize}
\item[\textsuperscript{185}] Barkham (2001), p 89.
\item[\textsuperscript{186}] Barkham (2001), p 89.
\item[\textsuperscript{187}] Barkham (2001), p 93.
\item[\textsuperscript{188}] Kerschischnig (2012), p 135.
\item[\textsuperscript{189}] Kerschischnig (2012), p 135.
\item[\textsuperscript{190}] Shackelford (2009), p 231. See also Shackelford (2014), p 289.
\item[\textsuperscript{191}] Boothby (2013), p 389.
\item[\textsuperscript{192}] Boothby (2013), pp 389-390.
\item[\textsuperscript{193}] Roscini (2014), p 55.
\end{itemize}
\end{footnotesize}
Roscini cites Schmitt’s position that generally this will not be the case, except perhaps where the data is ‘designed to be immediately convertible into tangible objects, like banking data’. Kerschischnig takes a similar position by suggesting that the time might be ripe for the law of armed conflict to realize that even non-physical damage can be so severe that it parallels physical damage inflicted by conventional weapons. This would require the inclusion of intangible property and a redefinition of the notion of “destruction” – in short, a significant shift in the use of force paradigm. The signs of the times clearly point to the integration of data under the notion of property – at least such that represents intangible assets that are directly transferable to tangible assets (e.g. funds, stocks, financial transactions).

He therefore argues that the notion of damage should be extended to intangible property too, at least where it has a direct link to tangible assets. Especially as a use of force does not necessarily rise to an armed attack and therefore does not always require actual violence. He writes that: ‘since a use of force can be assumed as soon as destruction of property occurs, the destruction of data arguably constitutes a use of force, even if no violence is involved.’ He maintains that the effect of this would be that cyber attacks aimed at directly destroying data are incorporated into the prohibition on the use of force. However, this would exclude mere cyber intrusions and cyber espionage as they only modify and manipulate data. As such, most authors within the literature note the how the harm that cyber attacks cause is problematic. This is especially where cyber attacks only have non-material effects and the harm that they cause does not easily fit within the law on the use of force. Nonetheless, the general position remains that unless a cyber attack causes material effects such as injury or death to human beings or damage or destruction of physical property, then it cannot amount to a use of force.

Section 2: Cyber Attacks and Non-Intervention

In the literature on cyber attacks and the use of force and non-intervention, like within the general literature on these principles discussed in part one, those measures not constituting armed force are considered unlawful interventions instead, provided the element of coercion

---

197 Kerschischnig (2012), p 137.  
198 Kerschischnig (2012), p 137.
is present. While not as much scholarly attention has been given to considering cyber attacks below the use of force that would be in breach of the non-intervention principle, as the focus has been on Article 2(4),\textsuperscript{199} most nonetheless maintain that the principle is applicable. There is a tendency to consider the non-intervention principle, in the context of the use of force analysis, as a secondary category into which to push the problematic cyber attacks that do not easily fit with existing understandings of what constitutes armed force.\textsuperscript{200} A notable exception to this however, is Russell Buchan who, focusing particularly on cyber attacks below the use of force, argues that:

\begin{quote}
the principle of non-intervention establishes a legal framework that can protect States from cyber attacks which, although not producing physical damage and thus not qualifying as an unlawful use of force, nevertheless have the effect of coercing a State into adopting a course of conduct that it is freely entitled to determine itself.\textsuperscript{201}
\end{quote}

Most however, do not devote as much attention to this principle as the non-use of force principle, and essentially maintain that those cyber attacks below the use of armed force can constitute interventions provided they are coercive. Roscini for instance argues that cyber attacks not producing destructive consequences or severely disrupting critical infrastructure ‘may be unlawful interventions in the internal affairs of other states, but are not a use of force.’\textsuperscript{202} He maintains there is no difficulty in qualifying cyber attacks as breaching the non-intervention principle when used ‘to coerce another State in order to obtain from it the subordination of the exercise of its sovereign rights and to secure from it advantages of any kind’.\textsuperscript{203} Similarly, Dinniss argues that cyber attacks with minimal effects or not manifesting in the physical sphere, but nonetheless warranting concern about whether they amount to force or not, will likely be considered as unlawful interferences instead.\textsuperscript{204} Joyner and Lotrionte also argue that cyber attacks that do not amount to force in the ‘literal sense … may be viewed as a form of intervention that can produce certain harmful or coercive effects in

\textsuperscript{199} As Buchan argues, even where scholars recognise the ‘potential application of this principle, they mention it only very briefly; crucially, these authors do not engage in a sustained analysis of how the non-intervention principle may apply to cyber attacks, particularly those falling below the threshold of an unlawful use of force.’ Buchan (2012), p 221.

\textsuperscript{200} Marco Benatar for example writes that ‘even if a cyber attack does not amount to a use of force, it is still an intervention, which constitutes a violation of international law.’ Benatar (2009), p 395.

\textsuperscript{201} Buchan (2012), p 226.

\textsuperscript{202} Roscini (2014), p 115.

\textsuperscript{203} Roscini (2014), p 65 citing the Declaration on Principles of International Law Concerning Friendly Relations and Co-operation among States in Accordance with the Charter of the United Nations (adopted by the UN General Assembly on 24 October 1970, UN Doc A/RES/2625(XXV)).

\textsuperscript{204} Dinniss (2012), p 74.
Mary O’Connell also emphasises that even though a cyber attack does not amount to a use of force, international law nonetheless prohibits cyber attacks under the principle of non-intervention. Finally, the Group of Experts maintained that not all forms of interference constitute unlawful interventions and that cyber espionage and cyber exploitations without the element of coercion present do not breach the non-intervention principle. They took the view that this is the case even where such actions involve the breach of ‘protective virtual barriers’ such as firewalls and passwords. However, the Group of Experts did provide examples of coercive cyber operations that would amount to breaches of the non-intervention principle. These included: the manipulation of elections or public opinion during elections; the alteration of online news services in favour of a particular political preference and the spreading of false news; and the shutting down of online services.

Therefore, according to the prevailing view, those cyber attacks without material effects similar to those traditionally associated with uses of armed force cannot be considered uses of force. In contrast to these ‘easy cases’, the more difficult ones arise where cyber attacks do not have clear material effects akin to what is normally understood as ‘force’ within Article 2(4). Those cyber attacks below this threshold, provided the element of coercion is present, are instead considered as potential breaches of the non-intervention principle. It is argued that this distinction between cyber attacks with material and non-material effects is a result of the law’s ontologically constrained view of violence. Destructive cyber attacks with material effects resembling physical violence easily fit within the law’s conceptualisation of violence and consequently the law has the capacity to regulate cyber attacks with material effects. This is regardless of whether the harm or damage is inflicted through kinetic force, by non-kinetic weapons, destructively used non-military force, or indeed cyber attacks. In each case, the law is capable of recognising these as forms of violence within the law on the use of force. However, those cyber attacks without material effects fall outside the law’s conceptualisation of violence. Also, given the tendency to cast these cyber attacks as potential breaches of the non-intervention principle alone, they are effectively depicted as forms of non-violence. Therefore, it is argued that the novel harm

---

207 Commentary to Rule 10, Schmitt (2013b), p 44.
caused by cyber attacks without material effects is not adequately accounted for by the law. As such, while the law has the capacity to regulate cyber attacks with material effects through the law on the use of force, it lacks the capacity to adequately deal with non-material cyber attacks.

**Conclusion**

The following chapters will consider the threshold distinction between the non-use of force and non-intervention principles in relation to the 2007 cyber attacks against Estonia and the Stuxnet incident. As such, these chapters will illustrate the law’s ontological constraints and demonstrate how an informational approach offers a means to overcome these limitations. Prior to this however, it is worth briefly contextualising the notion of informational violence into existing accounts of cyber attacks and the non-use of force and non-intervention principles. As discussed in chapter 3, cyber attacks with non-material effects can be considered as a form of informational violence. To a degree this is similar to what some of the authors discussed above have suggested. Kerschischnig for example argues that data should be integrated into the concept of property that can be destroyed for the purposes of Article 2(4). \(^{210}\) Schmitt has also suggested that there may be a shift towards considering ‘data destruction as the functional equivalent of physical destruction for use of force characterization purposes whenever the destruction of the data severely disrupts societal, economic or governmental functions.’ \(^{211}\) However, viewing such harm as informational violence goes beyond simply equating the destruction of data to that of physical objects. An informational approach seeks to capture both the actual damage or destruction of data that cyber attacks can cause, as well as the way in which this harms the state entity. As such, on a more conceptual level, both cyber attacks with and without material effects can be seen as capable of harming the state as an information entity when they produce increases in entropy.

Therefore, as the first of two case studies, chapter 5 considers the use of mainly disruptive cyber attacks against Estonia in 2007. Despite the scale and duration of the attacks and the disruptions that they caused to Estonia’s government and civil society, the cyber attacks are generally not considered to have constituted a use of force. In other words, because the cyber attacks did not involve material damage they did not constitute a form of

\(^{210}\) Kerschischnig (2012), pp 135-136 (citations omitted).

violence that the law is capable of recognising. Thus the Estonia incident demonstrates the law’s limited view of violence and its consequent inability to adequately regulate non-material cyber attacks. Chapter 6 provides the second case study which considers the Stuxnet cyber attack against Iran. In contrast to the Estonia incident, as Stuxnet involved material damage to centrifuges, the law is capable of recognising it as a form of violence within the law on the use of force. However, the Stuxnet incident demonstrates that as a result of its ontological constraints, the law only provides a one-dimensional account of violence. This account lacks depth as it does not adequately account for the various non-material ways in which Stuxnet harmed Iran. Accordingly, these case studies will be used to illustrate the law’s ontological constraints and demonstrate how an informational approach provides a means to overcome these constraints.

Overall, this chapter argued that the threshold distinction between the non-use of force and non-intervention principles in relation to cyber attacks highlights the law’s ontologically constrained view of violence. As a result, while the law is capable of regulating cyber attacks with material effects, its capacity is limited particularly in relation to cyber attacks without material effects. Part one considered the parameters of the use of force and non-intervention doctrines and argued that the law embodies a limited view of violence requiring material damage or harm. Part two then considered these doctrines in relation to cyber attacks. It was argued that, while the law has the capacity to regulate cyber attacks with material effects, as a result of its ontologically constrained view of violence, it has a limited capacity to regulate non-material cyber attacks.
Chapter 5: Estonia

Introduction

In September 2007, in an address to the UN General Assembly, Estonia’s President stated that:

Cyber attacks are a threat not only to sophisticated information technological systems, but also to a community as a whole. … The threats posed by cyber warfare have often been underestimated since, fortunately, they have so far not resulted in the loss of any lives. … In addition to concrete technical and legal measures for countering cyber attacks, governments must morally define the cyber violence and crime, which deserve to be generally condemned just like terrorism or the trafficking in human beings.¹

A few months prior to when this statement was made, Estonia had become subject to a new form of violence. In April and May of 2007, Estonia became victim to what the head of the US diplomatic mission to Estonia at the time described as ‘the world’s first cyber attacks against a nation state.’² In the media the incident was widely described as a cyber war.³ The cyber attacks occurred in response to the Estonian Government’s decision to relocate a politically contentious war memorial statue. At first there were protests and riots in the streets of Tallinn by Estonia’s ethnic Russians however, soon after this the ‘rioting’ also spread to cyberspace. What resulted was various waves of cyber attacks that lasted over three weeks. These attacks targeted a range of websites including those of government departments and banks, as well as the servers of Internet Service Providers (ISPs). The attacks did not result in physical damage or injury to human beings, and were primarily disruptive as a range of services were rendered temporarily unavailable. Despite initial allegations by Estonian officials that Russia was responsible for the attacks, Russia has denied its involvement.⁴

This chapter uses the 2007 cyber attack incident in Estonia to argue that an informational approach offers a means through which to overcome the law’s ontological constraints that limit its capacity to recognise non-material cyber attacks as a form of violence. The chapter is made up of three sections. Section one provides a detailed examination of the 2007 attacks against Estonia. It also considers the methods used in the cyber attacks from a technological perspective and the harm that Estonia suffered, as well as the uncertainty faced by Estonian officials in characterising the cyber attacks. Section two then considers existing legal analyses of the cyber attacks against Estonia in light of the law on the use of force. It demonstrates how the law’s ontological constraints are evident in the mainstream interpretation of the law on the use of force and its application to the incident. Finally, section three adopts an informational approach to consider Estonia as an information entity that was subject to cyber attacks amounting to a form of informational violence causing entropy. Consequently, it is argued that an informational approach offers a means to overcome the law’s ontological constraints and recognise a broader spectrum of violence that states can be subject to and which can undermine an international legal order in which the containment of violence is central.

Section 1: Events

1.1 Background and Overview

The cyber attacks against Estonia occurred in the wake of the decision by the Estonian Government to relocate a Soviet era war memorial statue (the Bronze Soldier). Ultimately the statue was moved from a park in the Tallinn suburb of Tõnismägi to the Defence Forces Cemetery roughly two kilometres southeast from its original location. It was the decision to relocate the statue, as well as its actual relocation, that sparked the cyber attacks. The proposed relocation of the statue caused anger among Estonia’s ethnic Russians and their supporters in Russia. For the Russians, the statue was a memorial to the Soviet soldiers who died during World War II, whereas for Estonians it was a symbolic reminder of their

---

oppression under the Soviets. Preparations for the removal of the statue on 26 April were accompanied by protests which lead to violence and riots in the streets. The protestors were mostly Estonians of Russian descent who account for about a quarter of Estonia’s population. Given the events of 26 April, the government decided to relocate the statue the following day ahead of schedule. Protests were also held in Russia in response to the removal of the statue, where the Estonian embassy was barricaded and ambassadors were assaulted. Besides the protests, riots and violence on the streets of Tallinn, the ‘rioting’ also spread into cyberspace. Following this there were numerous waves of cyber attacks lasting over three weeks in total.

Estonia was particularly vulnerable to cyber attacks given the way it had embedded use of the Internet into public life. Everything from communications between the state and its citizens, officials and private sector, to voting, filing of taxes and storage of public records occurs in or through the Internet. Indeed, Estonia had legislated to make access to the Internet a human right for Estonians. With the Internet and its use heavily integrated into public life, Estonia was already in 2007 an extremely wired society even by European standards. Developments leading to this state of affairs began in the 1990s as a part of Estonia’s ‘Tiger Leap’ program resulting in the creation of what can be described as an ‘e-state’ (electronic state). This began with the push by banks to promote Internet based solutions in their business in order to reach Estonia’s rural population, and was fostered by the government’s efforts to provide wide ranging access to the Internet through free Internet stations.
Alongside these developments, a digital national population registry system was created which became integral to the state information system. The national population registry stored information about Estonians digitally, whereas the state information system, a service centred organisation, created a common service space allowing for the state to function in cyberspace.\textsuperscript{17} The network connecting these services, the ‘X-Road’, is described as the ‘invisible yet crucial environment that allows the nation’s various e-services databases, both in the public and private sector, to link up and operate in harmony.’\textsuperscript{18} Together, these interconnected systems provide the means through which state services and communications to individuals, the private sector and among public officials are streamlined and digitalised.

For example, in 2001 electronic identification cards (e-IDs) were introduced.\textsuperscript{19} These cards serve as digital access cards to their holders and enable secure access to online government services.\textsuperscript{20} The use of these cards is not limited to online and real world identification purposes only, as they provide a link to a person’s information stored in government databases. This enables people to file taxes, social security or other payment claims, and even in some instances vote online without the need to complete paper forms. Further, communication between the state and the people occurs through official Estonian email addresses which are given to every e-ID card owner.\textsuperscript{21} Where e-IDs provide the people with a key to this digital realm, the Estonian State Portal acts as a centralised online gateway through which these services can be accessed. This website is considered ‘a one-stop-shop for the hundreds of e-services offered by various government institutions.’\textsuperscript{22} Effectively, the government is largely dependent on the Internet for its administrative and governmental operations.\textsuperscript{23} Therefore, already by 2007 Estonia was an advanced state in terms of e-government and integration of the Internet into its people’s everyday lives. As the cyber attacks in the spring of 2007 demonstrated however, Estonia’s technological advancement

also proved a vulnerability effectively exposing its e-state to attack in and through cyberspace.

1.2 Events

Following the removal of the Bronze Soldier and the protests and riots that ensued, Estonia became subject to cyber attacks varying in intensity and sophistication, beginning in late April 2007 and lasting until the latter half of May 2007. By some accounts, the initial attacks began late on 26 April, the night prior to the removal of the statue.24 Other accounts regard the first attacks to have occurred in the early hours of 27 April.25 The first attacks are believed to have targeted the Minister of Foreign Affairs’ website, followed by attacks against a wide range of government websites.26 On 28 April for example, the websites including that of the Prime Minister, Parliament, Government, and Ministry of Foreign Affairs had been attacked and rendered unreachable to legitimate users.27 The methods used in these attacks will be described below, but as a generalisation, the attacks that took place between 26 April and 29 April are regarded as the technologically less sophisticated ‘emotional phase’ of the attacks.28 These attacks made use of quite simple techniques when compared to the more sophisticated attacks that, according to cyber security experts, began to occur on 30 April.29

The attacks continued periodically between 1 May and 8 May. On 2 May for example, one of Estonia’s newspapers was forced to cut off international access to its website due to the volume of traffic from the cyber attacks that it was facing.30 On 9 May however, a significant spike in the attacks occurred. This was expected by the Estonians because it is a politically significant date for Russians marking their victory over Germany in World War II.31 The attacks began at midnight Moscow time and were the highest in intensity and

duration of all the previous attacks.\textsuperscript{32} It is believed that a large botnet was hired for this attack wave.\textsuperscript{33} Between 9 May and 18 May, government websites continued to be subject to cyber attacks. Estonian banks were also increasingly targeted during this time, and for example Estonia’s largest bank was forced to shut down its online services for 1.5-2 hours on both 9 May and 10 May.\textsuperscript{34} By 18 May the last major attack had occurred, though banks continued to experience some minor interruptions.\textsuperscript{35} Table 1 below provides a summary of the dates, targets, methods and level of sophistication of the attacks.

Table 1: Timeline of attacks, methods and sophistication

<table>
<thead>
<tr>
<th>Date</th>
<th>Targets</th>
<th>Method of attack</th>
<th>Sophistication level</th>
</tr>
</thead>
<tbody>
<tr>
<td>26 April</td>
<td>Parliament, President and Prime Minister’s websites are hit (between 26-27 April).</td>
<td>Pinging and malformed web queries.</td>
<td>Less sophisticated methods and simple instructions for launching attacks found in online forums.</td>
</tr>
<tr>
<td>27 April</td>
<td>President, Prime Minister, Parliament and government ministries’ websites swamped.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>28 April</td>
<td>Most government websites are targeted.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>29 April</td>
<td>Media outlets’ websites are attacked (27-29 April).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>30 April</td>
<td>Domain Name System (DNS) and routers run by Elion repeatedly attacked between 30 April and 18 May.</td>
<td>Distributed Denial of Service (DDoS) attacks using botnets.</td>
<td>More sophisticated attacks given use of botnets.</td>
</tr>
<tr>
<td>1 May</td>
<td>Estonian Internet Service Providers (ISPs) ‘under sustained attack’ and forced to reboot their systems.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9 May</td>
<td>Websites including that of the Foreign Ministry.</td>
<td>Major banks also experienced sustained DDoS attacks from 9-11 May.</td>
<td></td>
</tr>
<tr>
<td>15 May</td>
<td>Websites of government institutions.</td>
<td>Estonia’s second largest bank, SEB Eesti Ühispank, was forced to shut down its web portal for 1.5 hours, though restoration of services took longer.</td>
<td></td>
</tr>
<tr>
<td>18 May</td>
<td>Government websites targeted, though regarded as final wave of attacks, as only smaller attacks continue against banks.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

36 According to some reports, 26 April 2007 is the date on which the cyber attacks began, see Landler and Markoff, ‘Digital Fears Emerge After Data Siege in Estonia’, The New York Times, 29 May 2007; Evron (2008), p 123.
40 Evron (2008), p 123.
41 Other reports indicate that the first cyber attacks occurred on 27 April 2007, see Ottis (2008), p 164; Tikk et al (2010); Rantanen, ‘Virtual harassment, but for real’, Helsingin Sanomat, 6 May 2007.
As this table demonstrates, overlapping information exists on the exact timing of the attacks on specific websites. However, a detailed picture is difficult to provide as much of this information is unavailable. Nonetheless over these weeks, a large number of Estonian websites had come under attack including the websites of the President, Prime Minister, Parliament, most government departments, political parties, media organisations, banks and ISPs. The attacks also targeted Estonia’s Internet infrastructure and information systems, such as the national DNS and the DNSs operated by various ISPs. They also affected the operation of government communication channels and caused slight interruptions to mobile networks as well as to the emergency services line. However, the critical information infrastructure of transportation and energy systems, for example, were not targeted.

### 1.3 Attack Methods

The cyber attacks that occurred in the immediate aftermath of the real world protests and riots made use of relatively simple methods when compared to the more sophisticated attacks that began to emerge on 30 April. The less sophisticated methods consisted of both pinging and malformed web queries. In simple terms, pinging is the improper use of a troubleshooting program that is used in Microsoft Windows operating systems. Pinging is generally used when troubleshooting Internet communication problems and can be done simply by entering a command into Windows’ ‘Command Prompt’. Doing so sends Internet Control Message Protocol (ICMP) packets to the target address with the expectation that it will reply (provided the connection between the two is working). This method can be exploited when a large number of requests are sent and the target computer has a significantly lower bandwidth than

---

57 Email from Liisa Tallinn, Communication Manager, Estonian Information System’s Authority, to Samuli Haataja, 26 February 2013 (on file with author).
63 ‘Marching off to cyberwar’, The Economist, 4 December 2008.
the combination of incoming requests, creating a Denial of Service (DoS). A DoS thus occurs when the target system is subjected to a volume of data that it cannot handle therefore disrupting the ability of legitimate users to access it or its functions. Files containing command lines allowing for automated commands were also made publicly available to attackers. The use of these files minimised the amount of manual command input required of users and further automated the process. Some websites were also hacked and defaced, for instance an apparent apology in Russian was posted on the website of the Prime Minister’s political party. Therefore, the early cyber attack methods used in the immediate aftermath of the removal of the statue were relatively simple when compared to the sophistication of the later attacks.

The more sophisticated attacks that began to appear on 30 April were Distributed Denial of Service (DDoS) attacks. A DDoS occurs when multiple computers are used to target one system simultaneously. This is achieved through the use of botnets. A bot (short for robot), is a program designed to perform a certain action when it receives a command. Bots can run in the background of compromised computers, waiting for commands from their controllers. A computer can be compromised and made into a bot (or a ‘zombie’) without the awareness of its legitimate user, usually with the use of malicious software such as a Trojan. A botnet in turn is a network of synchronised bots (a network of robots) performing the commands of their controllers. Hundreds of thousands of compromised computers were involved in the attacks, geographically located across 178 countries including the US, Vietnam, Egypt and Peru. The aim of the DDoS attacks was to use the collective force of

73 Bots commonly operate in Internet Relay Chat (IRC) client programs. IRC is a network of servers that relay text chat messages to each other or their users (clients) that are connected to an IRC server. See Mirkovic et al (2005), p 294-5.
74 Mirkovic et al (2005), p 62.
75 Trojans are malicious software ‘designed to reach a target stealthily and to be executed inadvertently.’ Calder and Watkins (2010). These computers can then be centrally controlled and form a botnet, see Evron (2008), p 124.
the botnet to subject the Estonian websites to a higher volume of data than they could handle, causing them to overload and become unreachable to legitimate users. From the information available on the volume of data used in the attacks against Estonia, most were either less than 10 megabits per second (Mbps) or between 10 Mbps and 30 Mbps and lasted less than an hour. However, some of the attacks were made up of a significantly larger amount of data, reaching over 90 Mbps and lasting more than 10 hours. While even 90 Mbps is relatively small on a global scale, it was sufficient to be effective against Estonia given the low amount of bandwidth it normally requires for its Internet infrastructure which is relative to the size of its population. In this context, the attacks over 90 Mbps were significant. The largest of these attacks occurred on 9 May, though they suddenly stopped the following day. It is believed that this is when the rental time for the specific botnet expired. A number of different methods of DDoS attacks were used, though their general aim was to prevent legitimate users from accessing the targeted websites and the services they provided. These different methods of DDoS attack are described below.

The majority of the DDoS attacks were ICMP floods. These have been described as among the oldest and simplest methods of attack. This occurs when the attacking computer sends requests with a forged return address (that of the target’s) to a number of computers. These computers believe it is a request from the target computer and therefore send their response to that computer and effectively flood it with responses. The result can be the same as a DoS.

Based on flow data from one of the attacks during the Estonian incident, we mapped where the traffic origins to geographic coordinates. The result quite clearly shows how widely distributed the attacks were sourced, namely from all over the world. In this case this particular attack was from a botnet. We do not think that this attack used source spoofing as all of the IP addresses in question mapped back to allocated netblocks and not unallocated IP address space, as is commonly seen when the attacks used spoofed or forged source IP addresses.

Nazario (2009), p 12.
80 Mansfield-Devine (2012).
85 Tulloch (2003).
User Datagram Protocol (UDP) flooding was also used which is a similar technique involving a different protocol to Transmission Control Protocol (TCP), in which the target computer is forced to produce a number of packets rendering it unavailable to legitimate users. When the target computer receives UDP packets on one of its ports, it is forced to ‘check to see if any of its programs are set up to accept incoming data on that port.’ Generally this will not be the case, thus it will reply with an ‘ICMP Destination Unreachable Packet.’ Ultimately, the target computer will be flooded with these packets and unable to process and respond to them all, thereby preventing legitimate users from accessing it. Further, the origin of these packets can easily be concealed (the Internet Protocol (IP) address from which they are sent is fake, that is, it is ‘spoofed’) making discovery of the attack’s origin even more difficult.

TCP SYN (synchronisation) floods were also used. This occurs within the context of the TCP three-way handshake procedure which is required for two hosts to begin communicating with each other. Generally, to establish an Internet connection with another IP address, one host sends a TCP SYN packet to that address. The receiver of the TCP SYN packet then responds with a SYN ACK (acknowledgment) to the original host. That host then sends an ACK in reply, completing the ‘three-way handshake’ and establishing a connection between the two. When used in the context of a DoS attack, the attacking computer sends TCP SYN packets to the target computer however, the return address is replaced with a non-existing, spoofed address. As a result, the target computer is left waiting for a response to its acknowledgment packets that it will never receive. When the number of these initial TCP SYN packets sent to the target computer is multiplied, the target computer continues to send out SYN ACK packets to non-existing IP addresses which will never respond.

86 Ottis (2008), p 165.
91 Tulloch (2003).
92 Tulloch (2003).
Attempts to hack into systems using the more complex Structured Query Language (SQL) injections were used, some of which were ‘met with success at non-critical sites.’

SQL injection is not a type of DoS, but a means of hacking into the system in order to obtain access to it. According to cyber security expert Jeffrey Carr, compared to a traditional DDoS attack, exploiting SQL injection vulnerabilities ‘require[s] only a handful of attacking machines to achieve the same effect.’ Further, he maintains that the ‘[d]iscovery and exploitation of these application-level vulnerabilities shows moderate technical sophistication, but more importantly, it shows planning, organization, targeted reconnaissance, and evolution of attacks.’

Limited information is available on this method of attack against Estonia or the details of which methods were used on specific websites.

1.4 Effects

Collectively, these attack methods were aimed at disrupting the functioning of the targeted computers and websites, and the services they provided access to. Some maintain that, while the economic effect of the attacks is difficult to estimate, given that both the public and private sectors were reliant on ICTs and digital communications, the daily operations of various organisations, including banks, government departments and small businesses, were seriously impaired. Other estimates quantify the economic impact of the attacks at between 27.5-40.5 million US dollars. The broader societal effect that resulted was from the lack of access to information. With government department websites and communication channels inaccessible, the usual means and forms of communication between the government and Estonians were temporarily impaired. Further, given the degree to which important public services were only accessible online, the attacks against the state portal had a ‘discernible effect’ for many people. Additionally, the attacks also affected the flow of information about the events to the rest of the world. Especially given that most media sites were among the first to come under attack, Estonia was unable to rely on the usual online means for distribution of information.

93 Ottis (2008), p 165.
95 Carr (2011), p 141.
96 Only Rain Ottis mentions the use of this method, see Ottis (2008).
98 Li (2013), p 200.
1.5 Estonian Defences

Estonia’s defences in response to the attacks came primarily from its Computer Emergency Response Team (CERT). This team involved cyber security experts from both the public and private sectors, many of whom volunteered their assistance and expertise. The team was also assisted by foreign CERTs and cyber security experts, and both NATO and US experts came to observe and assist in the situation. The success of these experts in rapidly and flexibly responding to the crisis (in terms of information sharing and decision making) was partially due to the existing personal relationships between these people enabling them to work closely together without the hindrances of inter-agency bureaucracy. For example, an online chat room was organised which provided a forum for information exchange between the various CERTs and cyber security experts across the region, also providing Estonian authorities with real-time information on the attacks. Some reports also add luck as a factor to their success in mitigating the attacks, given that a number of the cyber security experts were in Tallinn at the time due to a meeting among European network operators.

Among the technical measures taken by the CERT was to increase the bandwidth of Estonia’s state information system servers in order to handle a larger volume of traffic. They also sought to filter malicious traffic, for example all traffic originating from ‘.ru’ (Russian) Internet addresses. Other measures included applying security patches to update software, firewalling, attack detection systems and blocking access. Also in cooperation with ISPs, incoming traffic was filtered based on patterns that had been identified in the malicious traffic, and network operators were also contacted directly to request the blocking of the course of the traffic. According to leaked diplomatic cables, Estonia’s banks were better prepared at defending against the attacks than the government, given that they had the

---

103 Evron (2008), p 123.
appropriate procedures and defence measures in place due to the prevalence of cyber crime in the region.\textsuperscript{113}

1.6 Estonian Responses and Russian Involvement

The cyber attacks against Estonia marked the first time a state was subject to a large-scale cyber attack,\textsuperscript{114} amounting to what Estonia’s President later described as ‘Web War One.’\textsuperscript{115} While ultimately dealt with as a criminal matter, especially during the attacks and in their immediate aftermath, there was a degree of uncertainty in how to characterise this novel form of ‘cyber violence.’\textsuperscript{116} Estonia’s immediate responses to the attacks reflected a fear that Estonia was under a partially virtual attack originating from Russia. On 1 May, Estonia’s Minister of Foreign Affairs declared that ‘[t]he European Union is under attack, as Russia is attacking Estonia.’\textsuperscript{117} The attack was described as ‘virtual, psychological and real – all at the same time.’\textsuperscript{118} This was echoed the following day in a speech by the Prime Minister to the Riigikogu (the Estonian Parliament), who stated that the sovereign state of Estonia was ‘under a heavy attack.’\textsuperscript{119} According to the Minister of Foreign Affairs, the cyber attacks were being launched by cyber terrorists who were using Russian IP addresses to attack Estonian sites and the Russian government was helping create an environment of hostility towards Estonia through its involvement in a propaganda campaign run by Russian state owned television channels.\textsuperscript{120} The Minister of Foreign Affairs assured that the government

\begin{itemize}
\item \textsuperscript{114} Traynor, ‘Russia accused of unleashing cyberwar to disable Estonia’, The Guardian, 17 May 2007.
\end{itemize}
had ‘plenty of evidence to support all of these statements.’ The Prime Minister’s speech similarly placed the ongoing cyber attacks into the context of the real world events that had occurred. He made specific mention of the assault of Estonia’s ambassador to Moscow, the tearing of the Estonian flag at its Russian embassy, and calls made for a change of government by the delegates of the Russian Duma. In this context he claimed that Estonia’s sovereignty was under attack. Further, the Prime Minister said that Estonia had turned to the EU for immediate action as one its member states was under attack. On 3 May, it was reported that Estonia’s President had also spoken to the NATO Secretary General who had ‘expressed serious concern about Russia’s behavior toward its neighboring state.’

Soon after these initial responses, Estonian officials moved away from describing the incident as an attack on its sovereignty. On 11 May the Minister of Foreign Affairs spoke at a Council of Europe committee meeting about the ongoing incident. While he continued to make reference to ‘evidence that these [cyber] attacks are well-coordinated and a significant amount of them originate from Russia’, he framed this within the language of cyber crime and the Convention on Cybercrime framework. For example, the Minister of Foreign Affairs stated that ‘[c]urrent developments clearly confirm that we need to combat cyber crime in co-operation and international understanding’ and further, he strongly urged Russia to take measures against cyber criminals operating within its territory due to the wider security threat that they pose. It was also reported that Estonia’s Minister of Defence attended a meeting of EU defence ministers in Brussels on 14 May. The ministers discussed the need for rapid

responses to future cyber attacks. In the lead up to the meeting, Estonia’s Minister of Defence made a statement raising issues with whether cyber attacks can constitute military action under the NATO framework which would allow for the invocation of the North Atlantic Treaty’s collective security provisions. In this context, he stated that ‘not a single NATO defence minister would define a cyber attack as a clear military action at present; however, this matter needs to be resolved in the near future.’ Yet the Minister of Defence is reported to have stated prior to the meeting that the incident ‘cannot be treated as hooliganism, but has to be treated as an attack against the state’. A day after the meeting, the Estonian Minister of Defence compared the attacks to terrorism stating that, given the ‘scale of damage and the way these cyber-attacks have been organised, we can compare them to terrorist activities’. Additionally, the following month (June 2007), the Minister of Defence explicitly identified the problem of classification stating that: ‘[i]n our minds, what took place was cyber-warfare and cyber-terrorism.’

Despite these allegations of Russian state involvement, ultimately the only person officially held responsible has been a twenty year old Estonian student who was fined for launching an attack against one of the targeted websites. Though Estonian officials had managed to track some of the attacks to Russian IP addresses (the assumed location of the computers), they lacked definitive information about the identity of the attackers (the identity of the people physically accessing those computers or doing so virtually from a different geographical location). For example, in response to Estonia’s accusations of Russian involvement, a Russian official suggested that its IP addresses could have been used by professional hackers in an attempt to ruin relations between the two countries.

cyber security expert assisting Estonia in the situation noted that anyone could have been using a computer located there, ‘from the son of some ministerial janitor upwards.’

As such, the prevailing view among experts is that no state actor, such as a Russian security agency, was responsible for the attacks, but instead that they were carried out by politically motivated non-state actors. However, and adding to the uncertainty, in March 2009 a member of the Russian Duma maintained that his assistant, a member of a pro-Russian youth group, was responsible for launching the attacks with his associates. This was consistent with some reports in 2007 that this group had admitted its involvement in the attacks. Some note however, that this account only explains some of the attacks used against Estonia. Others suggest that despite the lack of concrete evidence to prove Russian involvement, given a range of factors relating to the timing, volume and organisation of the attacks, the only plausible explanation is that Russian officials gave some degree of approval for the actions of those conducting the cyber attacks. Again other experts maintain that it is impossible to prove who was or was not responsible for the attacks based on the technical information available.

Therefore, the relocation of the Bronze Soldier triggered the cyber attacks against Estonia that lasted over three weeks in total. The cyber attacks were inherently informational – they did not result in damage to physical objects or injury to human beings. Nor were they conducted by human actors wielding kinetic weapons. The sophisticated DDoS attacks in particular involved unknown human actors controlling synchronised networks of robots, and the effects were primarily felt by Estonia’s Internet infrastructure and information systems.

141 Ottis (2008).
The attacks were therefore mainly disruptive, impairing the functionality of a range of computers and services that were closely connected to the daily operation of Estonia’s government and civil society. Given the uncertainty in how to characterise the attacks and whether (or to what degree) there was official Russian state involvement, the incident demonstrated the novelties of this new form of ‘cyber violence.’

**Section 2: The Ontological Constraints of the Law**

The Estonian incident highlights how ICT dependent information societies such as Estonia are also increasingly vulnerable to cyber attacks. It is a useful case study to consider the types of harm that states can be subject to in and through cyberspace, and how cyber attacks challenge the understanding of violence embodied in existing law regulating interstate violence. As demonstrated in previous chapters, the law on the use of force embodies an ontologically constrained view of violence. The law seeks to protect the state as a territorial entity from physical violence, such as the use of kinetic weapons or non-kinetic weapons with similar effects, resulting in damage or destruction of physical objects or injury or death to human beings. As was also shown, in much of existing literature on cyber attacks and the use of force, the dominant position is that cyber attacks will only amount to a use of force where they have material effects resembling those of conventional uses of force. Otherwise, cyber attacks cannot properly be considered uses of force and only potential breaches of the non-intervention principle. Therefore, drawing on the Estonia incident, this section argues that the law’s ontological constraints limit its capacity to recognise the cyber attacks against Estonia as a form of violence. However, as the Estonia incident demonstrated, even cyber attacks without material effects can constitute a form of informational violence capable of disrupting the functioning of increasingly ICT dependent states.

The cyber attacks against Estonia are widely discussed in international legal scholarship to highlight a non-hypothetical example of a cyber attack against a state and the various legal questions that cyber attacks raise. A prominent issue raised by the Estonia

---

incident was whether attacks of this kind could cross the use of force threshold and therefore amount to a use of force prohibited by the law.\textsuperscript{145} As will be illustrated by these analyses of the Estonia incident and the law on the use of force, the prevailing position is essentially that because the cyber attacks did not result in physical damage the incident cannot be viewed as a use of force under existing law. As a result, the Estonia incident is considered as potentially in breach of the non-intervention principle. In other words, the harm that resulted from the attacks did not fit with the law’s conceptualisation of violence, meaning the incident is instead depicted as a form of non-violence within the realm of the non-intervention principle. Therefore, it is argued that, due to its ontological constraints, the law lacks the capacity to recognise non-material cyber attacks as a form of violence capable of harming the state. This is despite the increasing ways in which non-material cyber attacks can disrupt the functioning of increasingly ICT dependent states, as illustrated by the attacks against Estonia.

2.1 Estonia and the Use of Force Threshold

Under existing law, Estonia would not qualify as a use of ‘armed force’ as prohibited by Article 2(4). The issues surrounding whether any such use of force was in the ‘international relations’ of states, that is, between state actors, and related issues surrounding state responsibility will not be considered here. In relation to the Estonia incident in particular, these issues revolve around whether the actions of non-state actors, acting under what is believed to have been at least tacit approval from Russian officials, can be attributed to a state under the state responsibility doctrine.\textsuperscript{146} As such, focusing only on the notion of ‘force’, generally the cyber attacks are not considered to have crossed the use of force threshold particularly because they lacked material effects. Exemplar of this position is, for instance, Russel Buchan who argues that because the cyber attacks against Estonia did not cause any physical damage and were merely disruptive, they cannot amount to a use of force: ‘a violation of Article 2(4) will only occur where a weapon is used that produces physical damage.’\textsuperscript{147} Therefore, he argues that ‘in the absence of physical damage … the cyber attacks

\textsuperscript{145} Among the authors expressly taking a view on this are: Schmitt (2011a), p 577; Buchan (2012), p 219; Gill and Ducheine (2013), pp 458-459; Li (2013), p 182.
\textsuperscript{146} On the issues surrounding state responsibility and cyber attacks, see for example Shackelford and Andres (2011), pp 984-993.
\textsuperscript{147} Buchan (2012), p 219.
committed against Estonia cannot be regarded as an unlawful use of force for the purposes of Article 2(4).\textsuperscript{148}

Michael Schmitt also maintains that under existing law the cyber attacks against Estonia would not amount to a use of force – however, in discussing the Tallinn Manual criteria he argues that they could amount to such or at least that this is likely the direction into which the law will develop.\textsuperscript{149} In other words, he maintains that under existing law the cyber attacks against Estonia would not amount to a use of force, but that under the Tallinn Manual criteria they could be viewed as such, or that the law may develop into the direction that they would. In discussing the Tallinn Manual criteria, he writes in relation to 1) the severity of the incident, that while no deaths, injury or physical damage resulted, the attacks ‘fundamentally affected the operation of the entire Estonian society.’\textsuperscript{150} This was evident in the severe disruption of government functions and services, and the negative effects on the economy and the daily life of Estonian people.\textsuperscript{151} As to 2) the immediacy of the consequences, he maintains that for instance the impact on the confidence in government and economic activity was more than merely an inconvenience and had an immediate effect that was widespread and long-term.\textsuperscript{152} The consequences of the attacks were also 3) direct as people were unable to access funds and government benefits, and 4) invasive because some of the targeted systems were designed to be secure.\textsuperscript{153} In relation to 5) measurability, Schmitt maintains that it is hard to quantify this because the consequences mainly involved denial of service opposed to the destruction of data.\textsuperscript{154} Finally, in relation to 6) presumptive legitimacy (assuming criterion 7) Russian responsibility is satisfied),\textsuperscript{155} he maintains that the attacks were more than political or economic pressure (which would fall outside the traditional use of force analysis) as they ‘involved intentionally frustrating governmental and economic functions.’\textsuperscript{156} Therefore, considering the Tallinn Manual criteria in relation to the Estonia incident, he argues that using this approach, the cyber attacks collectively would amount to what is regarded (or

\textsuperscript{148} Buchan (2012), p 219.
\textsuperscript{149} Schmitt (2011a), p 605. As mentioned in chapter 4, Schmitt originally developed the criteria which were later adopted into the Tallinn Manual. For the purpose of clarity, they will be referred to in the following discussion as the ‘Tallinn Manual criteria’. Therefore, where the work of other authors who have referred to the ‘Schmitt criteria’ is discussed, the term ‘Tallinn Manual criteria’ will be used in substitution (unless it is a quotation from these authors).
\textsuperscript{150} Schmitt (2011a), p 577.
\textsuperscript{151} Schmitt (2011a), p 577.
\textsuperscript{152} Schmitt (2011a), p 577.
\textsuperscript{153} Schmitt (2011a), p 577.
\textsuperscript{154} Schmitt (2011a), p 577.
\textsuperscript{155} Schmitt (2011a), p 577.
\textsuperscript{156} Schmitt (2011a), p 577.
should be regarded) as a use of force by the international community.\textsuperscript{157} However, he emphasises that these criteria only suggest the probable direction into which the law will develop in the future, but that the position in existing law remains intact.\textsuperscript{158} Therefore, under existing law, according to Schmitt, the cyber attacks against Estonia would not amount to a use of force.

Others cast doubt as to whether even under the Tallinn Manual criteria the Estonia incident could be considered a use of force, effectively reinforcing the mainstream interpretation of existing law and therefore that it would not capture the Estonia incident. In relation to the cyber attacks against Estonia and their analysis in light these criteria, Nicholas Tsagourias for example maintains that:

\begin{quote}
Their severity (in view of the duration and scope of the attack) was limited, and their harmful effect was limited and containable; the invasiveness of the attack was superficial and whereas there were some direct consequences, other consequences — economic or financial — were rather remote.\textsuperscript{159}
\end{quote}

Similarly, others argue that the Estonian incident would not amount to a use of force even under the Tallinn Manual criteria. One author for instance maintains that the ‘severity’ of the cyber attacks against Estonia falls short of a use of force as the consequences were minimal and ‘[t]here was no physical damage or measurable suffering.’\textsuperscript{160} Therefore, according to the position of these authors who do not consider the Estonia incident a use of force even under

\begin{flushleft}\footnotesize\textsuperscript{157} Schmitt (2011a), p 577. \textsuperscript{158} Schmitt writes that: the seven criteria proffered above in the use of force context can serve as useful indicators of whether states are likely to characterize particular cyber operations as armed attacks (or as initiating an armed conflict), and thus suggest the probable vector of the law. However, for the moment the existing law remains intact. Schmitt (2011a), p 605. \textsuperscript{159} Tsagourias (2014), p 25. \textsuperscript{160} Gervais (2012), p 540. Michael Gervais writes that: Under Schmitt’s criteria, the severity of this cyber attack falls short of the use of force. While the cyber attacks were immediate, the consequences were minimal. There was no physical damage or measurable suffering. The disruptions mostly caused a temporary inconvenience. The disruption of web traffic caused by the attack was indirectly related to the likely intended coercive effect, which was to reverse the Estonian government’s decision to remove the statue. The attack was intrusive and presumptively illegitimate, but the net results did not sufficiently resemble the use of force. Gervais (2012), p 540. Gervais however, goes on to discuss the cyber attack disrupting emergency services and maintains that this specific incident should amount to a use of force under the Tallinn Manual criteria.\end{flushleft}
the Tallinn Manual criteria, it is implicit that they do not consider it a use of force under existing law.¹⁶¹

Some authors also note the limitations of existing law, and develop alternate arguments to suggest that the cyber attacks against Estonia would constitute a use of force. Sheng Li maintains that instead of searching for the kinetic effects of a cyber attack, it is more appropriate to consider the wider consequences of a cyber attack and whether it threatens the state’s right to survival.¹⁶² He likens the cyber attacks against Estonia to naval blockades that, instead of restricting the flow of physical goods, restrict the flow of information. He writes that:

While it may have been true in the past that information blockades do not threaten the welfare of a state or its inhabitants as much as physical blockades, this is no longer the case in modern societies, in which individuals are heavily dependent upon access to digital information for their physical and material well-being.¹⁶³

Therefore, he maintains that given Estonia’s reliance on ICTs to the point that it was perhaps the most vulnerable state to such an attack,¹⁶⁴ and because at least a foreseeable consequence of the attacks was that Estonia’s critical infrastructure would be compromised,¹⁶⁵ the DDoS attack amounted to an armed attack (and consequently also a use of force).¹⁶⁶ As such, he takes the position that while not causing any physical effects, cyber attacks such as those against Estonia, can constitute uses of force where they seriously jeopardise the wellbeing of a state.¹⁶⁷ Under this view, not only would the cyber attacks against Estonia constitute a use

¹⁶¹ One author notes the malleability of the Tallinn Manual criteria, claiming they can easily be used to argue either for or against the position that the cyber attack against Estonia amounted to a use of force. See Nguyen (2013), p 1123. She writes that:
(1) the cyber attacks were not very severe because no one was physically injured, no property was damaged, and the DDoS attacks prevented users from accessing websites for generally no more than a few hours; (2) consequences ranging from decreased confidence in government to lost business resulting from inaccessible websites were delayed; (3) these effects were indirect consequences of the DDoS attacks, compared to the direct effect of lost server availability; (4) the attacks were executed remotely and involved no physical, territorial penetration; (5) the consequences are difficult to quantify because no concrete injury or damage occurred; and (6) the attacks were presumptively legitimate because they merely interrupted communications systems, which, under the U.N. Charter, is not considered “force.”

Nguyen (2013), pp 1123-1124 (citations omitted).

¹⁶² Li (2013), p 191.
¹⁶³ Li (2013), p 196.
¹⁶⁴ Li (2013), p 200.
¹⁶⁵ Li (2013), p 201.
¹⁶⁶ Li (2013), p 182.
¹⁶⁷ Li (2013), p 181.
of force, but they would even rise to the level of an armed attack legitimising the use of force in self-defence. Again implicit in this view is that under existing law on the use of force the cyber attacks against Estonia do not constitute a form of violence that the law recognises.

As the cyber attacks against Estonia are considered below the use of force threshold mainly because no material harm or destruction was caused, the incident is treated as a potential breach of the non-intervention principle. Accordingly, the incident is effectively likened to a form of non-violence. Buchan for instance argues that even though no physical damage was caused, given the duration and severity of the attacks, they ‘crossed the threshold of exerting influence and amounted to the intentional application of coercion against the Estonian government, seeking to force it to reverse its policy to relocate the statue of the Bronze Soldier.’168 Therefore, he maintains that the cyber attacks constituted a violation of Estonia’s sovereignty and breached the non-intervention principle.169 Tsagourias takes a similar position, arguing that even if the attacks were not a use of force, ‘they could amount to unlawful intervention because their aim was to change the Estonian government’s decision to relocate a Soviet era statue, provided however that they were attributed to a state.’170 Similarly, Anders Henriksen maintains that while the incident did not reach a threshold triggering the right to self-defence,171 if Russia was responsible and ‘intended to coerce the Estonian politicians to undo their decision to remove the war memorial’ then it would amount to a breach of the non-intervention principle.172 Consequently, because the cyber attacks, despite their duration and severity, did not cause material damage, they cannot be regarded as a use of force under existing law. Instead, they are at best viewed as a breach of the non-intervention principle.

In making this distinction primarily on the basis of the whether or not the cyber attacks had material effects such as damage to physical objects, these legal analyses of the Estonia incident reveal the law’s ontological constraints. This ontologically constrained view of violence means that under existing law on the use of force disruptive cyber attacks like those against Estonia cannot be sufficiently recognised by the law. Instead, because they failed to cause direct material effects such as the destruction of physical objects or injury to

human beings, the attacks are effectively equated to a form of non-violence outside the law on the use of force. Arguably these limitations are also recognised by authors like Schmitt and Li above, who seek to make arguments for how the cyber attacks against Estonia could be considered a use of force, or at least that the law should develop in that direction. As Schmitt notes in his analysis of the Tallinn Manual criteria outlined above, the cyber attacks had a fundamental impact on the functioning of Estonian society as governmental functions, services, and the daily lives of Estonians were disrupted. For Li in turn, the cyber attacks resulted in an informational blockade that impacted on the material wellbeing of Estonians. In both of these accounts the disruptive nature of the attacks is highlighted in contrast to the need for material destruction that pervades the view of violence embodied in existing law. As a result of the limited view of violence within existing law however, disruptive cyber attacks that are capable of undermining the proper functioning and wellbeing of states escape the doctrinal and conceptual bounds of the law seeking to regulate interstate violence. As the next section will demonstrate, an informational reconceptualisation of violence offers a means to overcome these constraints and also consider non-material cyber attacks as a form of informational violence capable of harming increasingly ICT dependent states.

**Section 3: An Informational Approach**

This section considers the cyber attacks against Estonia through an informational approach. This approach provides the means to consider and assess the impact of the attacks in the informational environment in which Estonian government and civil society functioned. As demonstrated in chapter 3, the state entity can be seen as an information system, and its ultimate purpose is to care for and protect the wellbeing of the entities within its region of the infosphere. In light of this reconceptualisation of the state, this section will first describe the Estonian entity as an information system. It will then consider the cyber attacks against the Estonian entity in April and May of 2007 in terms of the entropy they produced. Here it will be argued that particularly the DDoS attacks which disrupted the functioning of Estonia’s government and civil society, produced increases in entropy within the Estonian entity as an information system. In addition to infringing on its autonomy and its ability to interact, these attacks infringed on its essence as an entity by threatening its ability to care for and protect the entities within its region of the infosphere. It is argued that by reconceptualising violence through the notion of entropy and by considering states as information entities, the ontological constraints of the law regulating interstate violence can be reconfigured. This
enables recognition of non-material cyber attacks as a form of informational violence that states can be subject to – violence of a different nature but which is capable of disrupting the functioning of increasingly ICT dependent states.

3.1 The Estonian Entity

As a dynamic entity, in its usual state the Estonian entity is subject to continuous flows of information moving in and out of it. Within its region of the infosphere, approximately 82% of households have Internet access,\textsuperscript{173} there is a growing number of Internet users,\textsuperscript{174} the levels of access to ICTs are high, the ICT infrastructure is well developed, and there is a high level of use of ICTs across society.\textsuperscript{175} In terms of the economic impact of ICTs, the Estonian entity also ranks high globally reflecting a shift towards knowledge intensive activities in its economy.\textsuperscript{176} Similarly, there are continuous capital flows in and out of its economy.\textsuperscript{177} In addition to these information flows, when viewed informationally, all potential entities can be seen as information patterns or structures moving in and out of the Estonian entity’s region of the infosphere. As such, everything from the migration of humans to trade in goods can be seen as part of the changing flow of the informational substance of the Estonian entity. This entity is situated within a particular region of the infosphere – both in its territory and in the virtual environment of cyberspace. Therefore, particularly given its developed ICT infrastructure and the continuous flows of information that it continuously received, processed and communicated, the Estonian entity can be seen as a dynamic entity with a continuously changing informational substance.

The systematic features of the Estonian entity as an information system – its ability to interact, its autonomy, and its ability to adapt – delineated it as an entity from other entities.

\textsuperscript{173} International Telecommunication Union (2015), p 219.
\textsuperscript{175} The ITU’s ‘ICT Development Index’ (IDI) combines various indicators ‘to monitor and compare developments in information and communication technology (ICT) between countries and over time.’ International Telecommunication Union (2015), p 39. These indicators include the ICT readiness of the country (its level of networked infrastructure and access to ICTs), the ICT intensity (the level of ICT use in society), and the ICT impact (the outcomes of efficient and effective ICT use, or the ICT skills). International Telecommunication Union (2015), pp 39-41. In 2015 Estonia’s IDI was 8.05 (the highest being the Republic of Korea with 8.93) ranking it 20\textsuperscript{th} in the world. See International Telecommunication Union (2015), p 46.
Its autonomy as an information system, that is, its ability to act independently from other entities, was re-established in 1991 when it regained its political independence from the Soviet Union. As an entity it is capable of interaction – both with its internal sub-entities and sub-systems (humans, corporations, government institutions) and externally with regional organisations like the EU and NATO. Similarly, its ability to adapt as an entity and interact with other entities is highlighted by its decision to become a component of the larger EU information system, which it joined in 2004. Its adaptability is also highlighted by the measures it took in response to the cyber attacks, as will be shown below.

The form or pattern of the Estonian entity as an information system is evident in its information structures. Its unicameral parliament (the Riigikogu), Supreme Court and lower courts, executive government including the offices of the prime minister and president, and various government departments can all be seen as the informational structures according to which the Estonian entity as an information system was configured. While the humans occupying various positions within these sub-systems or components of the Estonian entity can change, as can their exact configuration, the persisting form or pattern of the organisation of these information structures delineated the Estonian entity.

The protocols governing the information exchanges between these components and other entities within the Estonian entity’s region of the infosphere come from its internal laws, policies and procedures. In addition to the constitution and other protocols configuring these sub-systems and their functions and tasks, there are also protocols according to which the people of Estonia can interact with these entities. In terms of the everyday operation of Estonia’s government and civil society, the information exchanges that take place involve a range of interactions between Estonian government institutions, the private sector and individuals. For example, since developments in the 1990s Estonia had increasingly moved towards a society in which the interactions between individuals and government occurred online.178 Government communications with its citizens, voting in elections, filing of social security applications, the filing of taxes, banking and so forth all increasingly occurred online, captured by the notion of ‘e-Stonia’ or ‘e-state’ that Estonia had become.179

relationship between Estonians and the government became one integrated with ICTs – by verifying their digital identities with e-IDs through computer interfaces Estonians could access various services linked to databases storing information about them, all connected by the X-Road or what is described as the ‘backbone of e-Estonia.’ These processes involve the interaction between various entities: humans, computer hardware and software, and public and private sector organisations. ICTs are at the core of these interactions, as are the various protocols enabling these interactions and the information exchanges between these entities. Therefore, these interactions between the sub-entities and sub-systems of the Estonian entity, operate according to the protocols that configure it as an information system.

The purpose of the Estonian entity as an information system is to care for and protect its region of the infosphere. Protecting its region of the infosphere means protecting itself as an entity from entropy from other entities, and caring for the wellbeing of this region to minimise increases in entropy. Consequently, its ultimate purpose as an entity is to protect the natural environment (from environmental pollution for example), its physical territory (from traditional military threats), and the virtual environment of cyberspace (from cyber threats such as DDoS attacks). Therefore, the flourishing or wellbeing of the Estonian entity as an information system depends on its ability to care for and protect its region of the infosphere, and its ability to prevent increases in entropy.

3.2 Entropy

Against this description of the Estonian entity as an information system, the harm caused by the cyber attacks can be viewed in terms of the increases in entropy that they produced. Unlike the usual information flows into the Estonian entity, the cyber attacks were different as they sought to disrupt the proper functioning of its government and civil society. As such, they constituted hostile information flows seeking to increase entropy within the Estonian entity. The cyber attacks produced entropy as they infringed on the Estonian entity’s ability to interact, its autonomy, and its very essence as an information system. However, the increases in entropy produced varied in degree when comparing the initial ‘emotional phase’ of the attacks to the later DDoS attacks.

See section one of this chapter. See also e-Estonia, ‘X-Road’, https://e-estonia.com/component/x-road/, accessed on 29 March 2016.
The ‘emotional phase’ of the attacks from 26 April to 29 April that involved unsophisticated methods such pinging and defacement of websites can be said to only have caused minor increases in entropy. These information flows primarily affected access to these sites and changed the content of some of these sites.\textsuperscript{181} These attacks did not disrupt the interactions between the components integral to the functioning of the Estonian entity, such as access to government services and banking, or the communications channels of government officials. As such, the impact of these attacks was minor in terms of infringing on the Estonian entity’s ability to interact and its autonomy, as mainly access to websites was affected. Also given the lack of sophistication in attack methods, the Estonian entity was easily capable of adapting to these attacks by increasing bandwidth for example. Similarly, these attacks did not significantly infringe on its ability to fulfil its purpose – to care for and protect the entities within its region of the infosphere. Therefore, while these attacks did cause some increases in entropy, these increases were only temporary and minimal and did not significantly disrupt the functioning of the Estonian entity as an information system. Also given its adaptability as a system, it was able to take measures to manage these information flows and prevent them from causing significant increases in entropy.

In contrast, the more sophisticated attacks resulted in more significant increases in entropy. Instead of merely rendering some websites inaccessible, these attacks impacted more significantly and widely on the Estonian entity’s informational infrastructure, impacting on the interactions between its components for a prolonged period of time. Consequently, these attacks impacted on the very essence of the Estonian entity as an information system, challenging its purpose as an entity, its ability to interact, and its autonomy, but demonstrating its adaptability as a system. The DDoS attacks involved hundreds of thousands of computers that had been compromised by malicious software. The properties of these entities had been corrupted, meaning they were able to be used as slaves to cause significant increases in the amount of information flowing into the Estonian entity. The corruption of these computers itself can be seen to have produced entropy on a global level, as it meant that the integrity of hundreds of thousands of entities had been undermined. However, only when this botnet was used against the Estonian entity, can it be said to have sought to cause entropy within the Estonian entity specifically. When used in the DDoS attack, the information requests that were sent by this collective of corrupted computers were aimed at disrupting the

\textsuperscript{181} For example, the website of the Prime Minister’s (Andrus Ansip) political party was hacked and an apparent apology in Russian was posted. See Tikk et al (2010), p 21.
functioning of the Estonian entity’s information infrastructure. As such, they were different to the legitimate requests that would come from human users seeking to use a single computer as a means to access and interact with websites or the information and services they provide access to. Instead of many individual users sending malicious requests to Estonian information systems like in the initial phase of the attacks, the virtually organised network of artificial entities allowed human users to significantly multiply the amount of information sent into the Estonia entity. The systematic and sustained flow of information that these attacks caused, resulted in more significant increases in entropy as they disrupted the Estonian entity’s proper functioning as an information system.

By exploiting a range of information exchange channels that normally enabled the natural flow of information in and out of the Estonian entity, the DDoS attacks subjected Estonian information networks to more data that, under normal conditions, it had the processing power and bandwidth to handle. These attacks impacted on the availability of services provided by various sub-systems, from banking to government emails, limiting human access to information and services, and preventing various computers and networks from functioning properly. As such, these attacks resulted in more significant increases in entropy than the ‘emotional phase’ of the attacks. They disrupted the availability of government and commercial services integral to the functioning of Estonian civil society, and therefore disrupted the functioning of the Estonian entity as an information system. For example, the DDoS attacks on 1 May that resulted in ISPs needing to reboot their systems, while only for 20 seconds, disrupted the functioning of a range of computer systems and the services they provided access to. This also affected human users reliant on the ISP for their Internet connection. Similarly, the attacks on Estonia’s largest banks – Hansabank on 9 May and 10 May, and SEB Eesti Ühispank on 15 May – required the banks to shut down online services for at least 1.5 hours on each occasion. While some of the attacks on a range of government websites throughout the first weeks of May lasted under an hour, many of them lasted up to five hours and some attacks lasted more than ten hours. Even though some of these attacks were short in duration, together they resulted in a sustained attack.

---

against government networks. For example, the Estonian Parliament’s email service was down for 12 hours as a result of the attacks. Similarly, the attacks disrupted the online availability of public services, particularly for Estonians overseas.

Collectively, the DDoS attacks that began to appear on 30 April and lasted into the second half of May, resulted in more significant increases in entropy than the initial ‘emotional phase’ of the attacks. While they did not cause any known material damage, they undermined the Estonian entity’s ability to interact, its autonomy, and its essence as an entity. Its autonomy in deciding the location of physical structures within its territory (such as war memorial statues) was challenged. The interactions of its internal components and entities within its region of the infosphere – including its citizens, government departments and services, and banking – were disrupted over numerous occasions for long periods in time, also affecting those Estonians outside of its region of the infosphere that were unable to access these services. These attacks also undermined the very essence of the Estonian entity as an information system, as the disruptions to the functioning of its government and civil society undermined its ability to care for and protect the entities within its region of the infosphere. Therefore, in contrast to the ‘emotional phase’ of the attacks, the DDoS attacks caused a more significant degree of entropy, disrupting the proper functioning of the Estonian entity.

The Estonian entity’s efforts to mitigate the effects of the attacks also demonstrated that as an information system it regarded these information flows as capable of increasing entropy, and that they needed to be minimised or prevented. Its ability to respond to the attacks however, also demonstrated its adaptability as an information system. A range of virtual entities such as software patches were utilised to remove vulnerabilities in computers, firewalls were set-up to filter and block malicious data, and attack detection systems were used to monitor and assist in detecting attacks. Similarly, by increasing server bandwidth, the Estonian entity was able to increase the capacity of its systems to function and thus prevent the increases in entropy that would have otherwise been caused by the high volume of traffic. Also, to prevent hostile data from entering the Estonian entity, large parts of its network were

---

closed to people outside its region of the infosphere, meaning Estonians overseas could not access their bank accounts\textsuperscript{187} or public services.\textsuperscript{188} As such, to preserve its own functioning and wellbeing as an information system, the Estonian entity to a degree disconnected itself from parts of the infosphere so that it could better protect the interactions between its internal components. All of these measures were taken in order to minimise and undermine the ability of the DDoS attacks to cause further increases in entropy within the Estonian entity as an information system. By taking these measures, the Estonian entity demonstrated that it was not operating under the usual conditions in which information flowed in and out of its system, but that it was being subject to information flows capable of causing increases in entropy. Additionally, through these measures, it sought to prevent further increases in entropy and protect its proper functioning as an information system. This in turn also demonstrated its adaptability as an information system.

Therefore, from an informational perspective, as a dynamic but systematic entity that is constituted by information structures and protocols, the Estonian entity can be seen an information system within its region of the infosphere. The cyber attacks that it was subject to in April and May of 2007 caused various degrees of increases in entropy. The DDoS attacks in particular, by disrupting the operation of government and civil society, constituted hostile information flows into the Estonian entity and undermined its ability to function properly. These attacks undermined its autonomy and ability to interact, and its inherent essence as an entity – as seen in the undermining of its ability to care for and protect its region of the infosphere.

\textit{3.3 Informational Violence and International Law}

Accordingly, an informational approach provides a means to reconsider the state as an entity subject to violence, and it allows for a reconceptualisation of non-material cyber attacks as a form of violence capable of harming the state entity. As the Estonia incident demonstrated, non-material cyber attacks are capable of disrupting the functioning of increasingly ICT dependent states by undermining their proper functioning as information systems. The cyber attacks undermined the Estonian entity’s ability to interact, its autonomy, and its capacity to

\textsuperscript{188} Tikk et al (2010), p 25.
care for and protect its region of the infosphere. Further, given the entropy the Estonia entity as an information system was subject to, its essence as an entity was degraded. As such, with state entities viewed in informational terms, even non-material cyber attacks can be seen as a form of informational violence. Therefore, for a state entity to be subject to violence, it does not necessarily need to be harmed in the form of material damage to physical objects or injury to human beings within its region of the infosphere.

This is in contrast to existing law on the use of force which, as demonstrated in section two, is ontologically constrained to recognising only forms of physical violence, as manifested in uses of armed force causing harm to human beings or damage to physical objects. The law is thus limited to regulating only certain forms of entropy that involve an entity’s material degradation or destruction. As the Estonia incident demonstrated, increasingly ICT dependent information societies can be subjected to novel forms of violence that, while capable of seriously disrupting the functioning of those societies, escape the central doctrines of international law regulating interstate violence. Had the cyber attacks directly caused damage to hardware or injury to human beings, they would have more readily fallen within the understanding of violence embodied in the law, and considered to have constituted a use of force under existing law. As this was not the case, the non-intervention principle is deemed applicable, meaning the incident is effectively depicted as a form of non-violence below the use of force threshold.\textsuperscript{189} However, making this distinction primarily on whether or not the attack in question results in material effects is artificial.\textsuperscript{190} As one of the

\textsuperscript{189} In contrast, as the examination of the Stuxnet incident in the next chapter will illustrate, the cyber attack against Iran’s uranium enrichment facility at Natanz is more readily considered a use of force under existing law especially due to the fact that nuclear centrifuges were physically damaged.

\textsuperscript{190} Li for example is also critical of this tendency in the literature to consider non-material cyber attacks as a breach of the non-intervention principle instead of Article 2(4), as it would essentially permit states to launch cyber attacks short of physical effects without triggering the consequences that flow from uses of force. See Li (2013), p 214. He writes that:

The effort to classify non-destructive cyber-attacks as interventions rather than uses of force in violation of Article 2(4) is even more destabilizing. While such a position means that reciprocal countermeasures would also not breach Article 2(4), it rests upon the premise that the acts of military officers launching information warfare operations from military computers against hostile networks overseas do not qualify as a use of military or armed force. This is reminiscent of the legal fiction of classifying the use of warships to blockade foreign ports as not warlike in order to legitimate pacific blockades. Because pacific blockades were merely interventions that did not trigger the legal consequences of war, Europeans nations with strong navies frequently resorted to naval blockades as an instrument of statecraft against weaker states. Similarly, if non-destructive cyber-attacks are merely interventions rather than illegal uses of force, we can expect "pacific cyber-attacks" to become a common instrument of statecraft for the strong to wield against the weak. This would create a technological loophole to the U.N. \textit{jus ad bellum} framework. Given the magnitude of harm, such attacks can cause, especially against small and wired societies such as Estonia, the consequences can be catastrophic for international peace and security.
central purposes of the UN Charter based legal order is the containment of interstate violence and conflict, an ontologically constrained, anthropocentric and materialist conception of violence limits the law’s capacity to recognise the informational violence that, as the Estonia incident demonstrated, can increasingly be real. Therefore, the law’s limited capacity to recognise a broader ontological spectrum of violence effectively undermines the law’s ability to contain violence.

Accordingly, an informational reconfiguration of the law’s ontological constraints makes it possible to also recognise non-material cyber attacks as a form of violence. By reconceptualising violence through the notion of entropy and viewing the state entity in informational terms, a broader ontological spectrum of violence can be recognised and also contained through law. This is warranted given that, as the Estonia incident demonstrated, cyber attacks highlight the changing nature of violence in a world of increasingly ICT dependent information societies that exist not simply in a physical, territorial space, but also virtually in cyberspace and as part of the infosphere. Yet non-material cyber attacks effectively escape the dominant legal doctrines regulating interstate violence, as evident in the depiction of such attacks as a form of non-violence below the use of force threshold. Instead, by adopting an informational approach the cyber attacks against Estonia can be regarded as constituting a form of informational violence against the essence of the Estonian entity. Therefore, through an informational reconfiguration of the law’s ontological constraints, a broader ontological spectrum of violence can be recognised.

Conclusion

This chapter used the cyber attacks against Estonia in 2007 as a case study to argue that an informational approach offers a means to overcome the ontological constraints of the law on the use of force. Section one detailed the events in Estonia in 2007 highlighting Estonia’s dependency on ICTs, the technical methods and effects of the cyber attacks, as well as the uncertainties evident in the characterisation of the cyber attacks among Estonian officials. The second section considered the Estonia incident in light of existing law on the use of force. Here it was demonstrated that the disruptive cyber attacks against Estonia largely fell outside existing law on the use of force primarily due to the lack of material damage caused by the attacks, highlighting the ontological constraints of the law’s conception of violence. Section three then adopted an informational approach to reconceptualise the cyber attacks as
a form of informational violence causing increased entropy within the Estonian entity. This was particularly evident in the undermining of the Estonian entity’s ability to interact, its autonomy, and its ability to care for and protect the entities within its region of the infosphere.
Chapter 6: Stuxnet

Introduction

In 2012 in Fordo, close to the city of Qom in northern Iran, an object that appeared to look like a rock exploded.¹ The examination of the object’s remains revealed that it was not a rock but instead a ‘device capable of intercepting data’ from the computers located at a nearby uranium enrichment facility in Fordo.² The origins of this device remain unknown however, media reports have linked it to similar technologies developed by the US National Security Agency (NSA) as revealed in the course of the Edward Snowden revelations.³ These technologies have the capacity to transmit data through radio frequencies from computers that are not connected to the Internet, provided they have been connected to hardware making this possible.⁴ Approximately 200 kilometres away from the Fordo uranium enrichment facility⁵ is the uranium enrichment facility of Natanz. This facility was at the centre of what was revealed to be a joint US and Israeli operation called ‘Olympic Games’.⁶ It was aimed at sabotaging the operation of Iran’s uranium enrichment facility in Natanz and involved a sophisticated piece of malicious software (malware) named by those who discovered it as Stuxnet.⁷ Originally discovered in June 2010,⁸ Stuxnet has been described as the ‘malware of the century’.⁹ It had managed to penetrate computer systems within Iran’s Natanz uranium enrichment facility that, like the computers at the aforementioned Fordo facility, were not connected to the Internet. Stuxnet’s design demonstrated that its ultimate aim was to adjust the frequency settings responsible for the rotation speeds of nuclear centrifuges, causing physical damage to the centrifuges and in effect undermining Iran’s ability to successfully enrich uranium. In contrast to the 2007 DDoS attacks on Estonia, Stuxnet was therefore not

¹ Mahnaimi, ‘Flintstone’ spy device explodes at Iranian nuclear site’, The Australian, 23 September 2012.
⁴ These technologies, in operation from at least 2008, rely ‘on a covert channel of radio waves that can be transmitted from tiny circuit boards and USB cards inserted surreptitiously into the computers.’ However, these transceivers have to be physically inserted into the computers, enabling them then to receive and transmit data through radio frequencies. See Sanger and Shanker, ‘NSA devises radio pathway into computers’, The New York Times, 15 January 2014.
simply aimed at disrupting the functioning of ICTs, but instead aimed at causing physical damage to nuclear centrifuges.

This chapter considers the Stuxnet incident to argue that an informational approach offers a means to appreciate the depth of the harm caused by Stuxnet. Despite the law’s ontological constraints which prevented the Estonia incident from being regarded as a use of force, the law has the capacity to recognise Stuxnet as a form of violence given the material damage to centrifuges it caused. It is argued however, that this is a one-dimensional account of violence as the focus is mainly on Stuxnet’s material effects. Instead, an informational approach offers a means to appreciate the informational and physical forms of violence that the Iranian entity was subject to and hence provides a deeper account of violence.

This chapter is divided into three sections. Section one provides a detailed examination of Stuxnet, including its technical design, overall purpose, and its effects on the nuclear centrifuges at Natanz. Section two then considers existing analyses of Stuxnet in relation to the law on the use of force. Here it will be demonstrated that, in contrast to the Estonia incident, Stuxnet is almost universally considered to have crossed the use of force threshold. Effectively Stuxnet constituted a form of violence that the law is capable recognising because it caused material damage to centrifuges. However, it is argued that the law, given its ontological constraints, only provides a one-dimensional account of violence that does not adequately capture the non-material harm that Stuxnet caused. Finally, the third section adopts an informational approach to consider the increases in entropy caused by Stuxnet against the Natanz system within the Iranian entity’s region of the infosphere. It is argued that by recognising both the informational and physical harm caused by Stuxnet, an informational approach offers a means to appreciate the depth of violence that the Iranian entity was subject to.

Section 1: Events

1.1 Media Reports
Stuxnet is the name given to a piece of malicious software that was first discovered in June 2010 by a Belarussian Internet security firm working for a client in Iran. Stuxnet was described as a ‘turning point’ in the design and purpose of malicious software. Unlike other computer viruses or worms that are commonly designed for financial gain for instance, Stuxnet was specifically designed for sabotage. It appeared that it was tailored to target the computer systems used to control important infrastructure, as the hardware and software configurations it targeted were those used to operate a range of industrial equipment found in power grids, power plants, pipelines and dams.

Initially the exact purpose of Stuxnet and who was responsible for its creation were not known when it was first discovered in June 2010. However, particularly given its technical sophistication, it was widely believed that simply a group of hackers could not have been able to create it, and instead that a nation-state was responsible for its development. Stuxnet’s design for example showed that its creation required a sophisticated team of programmers and an organisation with ‘substantial financial resources to develop, test and then release such a program.’ Similarly, in relation to its purpose, while later revelations in 2012 appear to confirm that the US and Israel had created Stuxnet to target Iran’s uranium enrichment facility at Natanz, the primary target or purpose of Stuxnet was not immediately known when it was first discovered.

Stuxnet was reported to have spread to computers across the world. According to Siemens, the manufacturer of the computers it ultimately targeted, Stuxnet was found in fifteen industrial plants around the world, five of which for instance were located in Germany. However, none of these sites’ operations were affected. Globally over 100,000

computers had been infected but over 60% of these were located in Iran.\textsuperscript{21} Iran therefore appeared to be the general or primary target of the attacks however, at first there was only speculation about the specific target of the attacks within Iran.\textsuperscript{22} For example, given reports that a computer worm had infected the personal computers of workers at Iran’s Bushehr nuclear plant, it was suggested that the Bushehr plant was potentially Stuxnet’s target.\textsuperscript{23} However, later analysis of Stuxnet’s code revealed that this was not the case.\textsuperscript{24}

In September 2010 there was already some speculation that the enrichment facility at Natanz was the target of the attacks.\textsuperscript{25} In November 2010, only days after it was revealed by the computer security company Symantec that Stuxnet targeted specific frequency converter drives operating in a very particular way, reports from the International Atomic Energy Agency (IAEA) noted that Iran had ‘stopped feeding hot uranium gas into its thousands of centrifuges’.\textsuperscript{26} As Iranian officials did not provide any reason for this, it led some to believe that it was as a result of the operators of the Natanz facility disconnecting computers and restoring systems to ensure that all traces of Stuxnet were removed.\textsuperscript{27} In late December 2010, the Institute for Science and International Security (ISIS)\textsuperscript{28} released a report in which it had compiled data from the IAEA’s quarterly reports on Iran.\textsuperscript{29} Combined with Symantec’s technical analysis of Stuxnet, these findings effectively confirmed that the Natanz facility was Stuxnet’s target and that Stuxnet was responsible for a fall in the number of working


\textsuperscript{24} According to Albright et al:

Contrary to several recent media reports, Stuxnet does not appear to be designed to attack the Bushehr nuclear power reactor. Stuxnet has spread easily on Windows-based computers, so it is not surprising that computers at other Iranian facilities, namely the Bushehr nuclear power reactor, would contain this malware. But the code’s attack sequences do not appear targeted at a nuclear power reactor or its associated systems.


\textsuperscript{26} Kessler, ‘Centrifuges in Iran were shut down, IAEA report says’, \textit{The Washington Post}, 24 November 2010.

\textsuperscript{27} Zetter (2014), p 237-238.

\textsuperscript{28} The Institute for Science and International Security is a non-profit think tank focused on issues surrounding the proliferation of nuclear weapons technologies.

\textsuperscript{29} Albright et al (2010).
centrifuges at the Natanz facility during late 2009 and early 2010. An estimated 900-1000 centrifuges were reported to have broken.31

In January 2011 the New York Times reported that Stuxnet was a joint US and Israeli effort targeted at the Natanz facility.32 The following year, in June 2012, the New York Times reported that the name of this operation was Olympic Games.33 Interviews with current and former US, European and Israeli officials revealed that Stuxnet was part of an operation which was originally started during President George W. Bush’s administration and later intensified under President Barack Obama’s administration. It had involved an extensive development program that required in-depth knowledge of the ‘structure and daily rhythms’ of the Natanz enrichment facility.34 Stuxnet also had to be tested at what was described as a ‘virtual replica of Natanz’ equipped with the same centrifuges (which were of an older design) as those used at the Natanz facility.35 According to these reports, given that Stuxnet needed to be physically introduced into the Natanz facility (that is, it could not be done across the Internet), they relied on engineers and maintenance workers with physical access to the facility for example, to unknowingly infect the computers therein.36 USB thumb drives were reported to have been ‘critical in spreading the first variants of the worm’, while more sophisticated methods were used to further spread and deliver the code to the computers it targeted. Originally Stuxnet was not meant to spread outside the computers at the Natanz facility, and this was attributed to an error in its code which was reported to likely have been a later modification by the Israelis.37

1.2 Technical Design

In addition to the media attention the incident received, the cyber security community also examined Stuxnet carefully. In late September 2010, the computer security company

35 Sanger, ‘Obama Order Sped Up Wave Of Cyberattacks Against Iran’, The New York Times, 1 June 2012. This was also reported the previous year, see Broad et al, ‘Israeli Test on Worm Called Crucial in Iran Nuclear Delay’, The New York Times, 15 January 2011.
Symantec released a dossier containing the company’s technical analysis of Stuxnet. Symantec had reverse engineered Stuxnet to properly understand its purpose and design. The final version of this dossier was released in February 2011 (version 1.4). By this time Symantec had gathered 3280 samples of Stuxnet in its three variants. Given that Stuxnet records a timestamp and other computer information, each sample had a history of every computer that it had infected. In addition to technical information about Stuxnet’s design and purpose, based on this data Symantec was also able to determine a range of factors including the different organisations Stuxnet had spread to and from, when these infections occurred, and how long it took to spread. In 2013 Symantec also released a follow up to its earlier report entitled ‘Stuxnet 0.5: The Missing Link’. Stuxnet 0.5 was the oldest known version of Stuxnet that had been analysed. It is believed to have begun its operation as early as November 2007, though it was designed to stop compromising computers on 4 July 2009 and stop communicating with its command-and-control servers already on 11 January 2009. Compared to the ‘full’ version of Stuxnet, Stuxnet 0.5 had some different and less developed features, and a different attack strategy. The full version of Stuxnet infected computers in three different attack waves: in June 2009, March 2010, and April 2010. Overall, Stuxnet’s technical sophistication was evident in a range of its features that enabled it to reach the facility at Natanz and deliver its payload to the computers used to operate the nuclear facility.

---

39 From the samples, Symantec identified three distinct variants of Stuxnet. The report mainly focused on the ‘March 2010’ variant as it is very similar to the ‘April 2010’ variant, and a newer version of the ‘April 2009’ variant. The report noted that a fourth variant is likely to exist too however, a sample of it had not been recovered. The newer versions/variants had additional features (more resources), were smaller in size, and had streamlined aspects of the update process. Approximately 98% of the samples collected were either the ‘April 2010’ variant (51%) or the ‘March 2010’ variant (47%). According to the report, the small amount of ‘April 2009’ variants may have been due to a slower infection rate, or it having been updated by newer versions of Stuxnet. See Falliere et al (2011), pp 53-54. The report noted that each variant formed part of a distinct ‘attack wave’, see Falliere et al (2011), p 8.
41 McDonald et al (2013).
44 For example, unlike the various propagation methods available to Stuxnet, Stuxnet 0.5 was only able to replicate itself through Step 7 project files on removable drives. It was also built on a different development platform, suggesting different developers were involved in the projects. Its attack strategy was different, as it was designed to attack valve systems, instead of modifying the speed of centrifuges. The connectivity functions of Stuxnet 0.5 to its command and control servers was also more limited, as it was only able to update itself through these means, and hence not provide ‘fine grained control’ to its operators. See McDonald et al (2013), pp 2-4.
centrifuges. Among these features were four zero-day vulnerabilities;\(^{47}\) two stolen digital certificates; multiple propagation methods enabling it to spread across computers not connected to the Internet; a sophisticated payload delivered only to computers configured in a particular way; the ability to disable digital alarm systems; and the use of a ‘man-in-the-middle’ attack to make it appear that its target computers were operating normally while it delivered its payload. These features will be examined in detail below however, what follows is first an overview of the international context of Iran’s nuclear program, and also the uranium enrichment process generally.

1.3 The Non-Proliferation Treaty and the Uranium Enrichment Process

Stuxnet’s ultimate goal was to undermine Iran’s ability to develop nuclear weapons. Under the Treaty on the Non-Proliferation of Nuclear Weapons (NPT)\(^ {48}\) regime which Iran is party to,\(^ {49}\) except for those states that had a nuclear weapons capability at the time in the late 1960s (the US, United Kingdom, France, Russia and China), other member states such as Iran are only permitted to use nuclear technology for peaceful purposes.\(^ {50}\) Additionally, pursuant to the NPT,\(^ {51}\) non-nuclear weapon states such as Iran have entered into safeguard agreements with the IAEA to ensure the transparency of their nuclear programs allowing the IAEA to monitor and verify their compliance.\(^ {52}\) Iran claims that its nuclear program is for peaceful purposes however, the US, other Western states, and also the IAEA maintain that Iran intends to develop a nuclear weapons capability.\(^ {53}\) For example, until 2002 the existence of Iran’s uranium enrichment facility at Natanz had not been disclosed contrary to Iran’s commitments under the NPT safeguard obligations,\(^ {54}\) and in 2003 the IAEA found traces of highly enriched

\(^{47}\) Kushner (2013), p 51. These are vulnerabilities in software unknown to the developers, meaning where such vulnerabilities are exploited, the developers of the software have ‘zero days’ (in terms of time) to develop fixes for the vulnerability.


\(^{49}\) Iran signed the NPT in 1968 and ratified it in 1970. On the history Iran’s nuclear program, see Bahgat (2006), pp 308-312.

\(^{50}\) Article IV of the NPT recognises ‘the inalienable right of all the Parties to the Treaty to develop research, production and use of nuclear energy for peaceful purposes’, and pursuant to Article II those states without an existing weapons capability agree not to by any means receive or develop nuclear weapons: Treaty on the Non-Proliferation of Nuclear Weapons, opened for signature 1 July 1968 [1973] ATS 3 (entered into force 5 March 1970).

\(^{51}\) Treaty on the Non-Proliferation of Nuclear Weapons, opened for signature 1 July 1968, [1973] ATS 3 (entered into force 5 March 1970), Article III.

\(^{52}\) Calamita (2009), pp 1399-1400.

\(^{53}\) Khan (2009), p 51.

\(^{54}\) Calamita (2009), p 1400; Bahgat (2006), p 310.
uranium at the Natanz facility. Consequently, the UN Security Council has through various resolutions authorised and imposed sanctions against Iran aiming to limit its capacity to obtain the technology and materials that contribute to its development of nuclear weapons technologies. Therefore, while Iran is permitted to develop, research, produce and use nuclear energy for peaceful purposes under the NPT, given the dual-use nature of this technology, the concern is that if it develops an effective ability to enrich uranium for peaceful purposes, it will also be able to further enrich uranium for weapons purposes.

The primary difference in the production process used to enrich uranium for either ‘peaceful’ or ‘weapons’ purposes is minor, lying ‘only in the extent and duration of the application of those processes to the uranium.’ The uranium enrichment process involves increasing the concentration of the uranium-235 (U-235) isotope which only makes up 0.7% of natural uranium. Uranium enriched for energy production requires about 3.5-5% of the U-235 isotope, and as this is below 20% purity it is regarded as low-enriched uranium (LEU). Where the concentration of U-235 is over 20% it is considered highly enriched uranium (HEU), whereas weapons grade uranium requires approximately 90% of U-235. Therefore, the uranium that can be used for energy or weapons purposes mainly differs in terms of the concentration of U-235. The process used to enrich uranium is also largely the same, as ‘[t]he essential difference in the production process for material of weapons grade purity, as opposed to reactor fuel purity, lies only in the extent and duration of the application of those processes to the uranium.’ There are also various methods of uranium enrichment however, the gas centrifuge process used at the uranium enrichment facility at Natanz involves large rotating cylinders (centrifuges) that are connected to form cascades (groups of centrifuges). The enrichment process involves feeding uranium in its gas form as uranium hexafluoride (UF₆) into the centrifuge which is being spun by a rotor inside. The rapid

57 Khan (2009), pp 51-52.
rotation of the UF₆ results in a higher concentration of U-238 (the unwanted uranium isotope which forms 99.3% of natural uranium) in the outer edge of the cylinder because of its heavier molecules.⁶³ This means the U-235 molecules are concentrated in the centre of the cylinder and they are drawn from one end of the cylinder.⁶⁴ Provided there is sufficient UF₆, this process can be used to enrich uranium for either energy or weapon purposes.⁶⁵

The centrifuge cascades (forming modules) used in the enrichment process are operated by special computers called programmable logic controllers (PLCs). A PLC is ‘controller that uses programmable memory to store instructions and to implement functions such as logic, sequencing, timing, counting, and arithmetic in order to control machines and processes.’⁶⁶ PLCs are not like personal computer systems with input devices such as a keyboard and mouse attached. Instead, they are computers of a special form that are ‘optimized for control tasks and the industrial environment.’⁶⁷ PLCs are programmed by engineers for example using personal computers such as laptops to input instructions into the memory of the PLC, and the PLC uses these inputs to carry out the functions for what it is programmed.⁶⁸ Siemens PLCs specifically are controlled with computers installed with Step 7 software. Using this software, a PLC can be programmed so that once the computer used to program it is disconnected, the PLC functions independently.⁶⁹ In the case of uranium enrichment, PLCs are used to configure the operation of the centrifuges cascades, including for example the speed at which the rotors inside the centrifuges are spun. Stuxnet’s goal was to first spread across personal computers with Microsoft’s Windows operating system installed, with the aim of reaching a computer used by an engineer or programmer to input instructions into the PLCs. Therefore, it first spread across these personal computers with the aim of eventually reaching the PLCs that were used to control the centrifuges.

1.4 Propagation Methods

---

⁶⁶ Bolton (2009), p 3.
⁶⁸ Bolton (2009), p 3.
The PLCs and the personal computers used to program PLCs are generally non-networked or ‘air-gapped’ meaning they are not connected to the Internet or even a Local Area Network (LAN).\(^70\) As such, to infect the computers used to control the centrifuges at Natanz, Stuxnet had to first be physically carried into Natanz on an infected computer or USB drive.\(^71\) It is unknown how or when Stuxnet 0.5 was introduced into Natanz.\(^72\) However, as the full version of Stuxnet included a record of the computers it had infected, it is known to have spread to Natanz from five separate Iranian companies understood to be involved with Iran’s nuclear program.\(^73\) A total of 12,000 infections were found in the computers of these companies from Stuxnet’s log file.\(^74\) It has been suggested that the original infection of Stuxnet to these companies’ computers could have been through a removable drive or an email attachment, by either an insider or an unsuspecting third party.\(^75\) Once the computer or USB drive of a contractor or programmer was infected with Stuxnet, it was capable of crossing the air-gap into the Natanz facility.

In order to spread across Windows computers in an effort to ultimately reach the PLCs, Stuxnet utilised numerous features. One way was through removable drives such as USB drives, and this was the main propagation method used.\(^76\) Stuxnet was able to copy itself onto a USB drive and hide the existence of its files on that drive. When the computer in question scanned the files on the USB drive, Stuxnet ‘intercepted the commands and served back a modified list that didn’t include Stuxnet’s files.’\(^77\) This way users could not notice that the removable drives contained Stuxnet, or that the removable drive was the source of the infection.\(^78\) The particular file used in this process used a stolen digital signature, meaning any Windows computer it reached would trust it as a safe file.\(^79\) This and the other digital signature used by Stuxnet were not forged, but stolen from two separate companies located in physical proximity to each other.\(^80\) In this process, Stuxnet also utilised a zero-day vulnerability in .LNK files allowing it to execute automatically when the icons are rendered

\(^72\) Zetter (2014), p 322.
\(^74\) Zetter (2014), pp 97-98.
once a USB drive is inserted.\textsuperscript{81} This way Stuxnet could spread onto other computers into which the USB drives were inserted. Once a removable drive had infected three computers, Stuxnet would delete itself from the removable drive.\textsuperscript{82}

Another way in which Stuxnet was able to spread across Windows computers was across a LAN using another zero-day vulnerability.\textsuperscript{83} The print-spooler vulnerability allowed Stuxnet to spread across computers that shared a printer over the LAN.\textsuperscript{84} Additionally, Stuxnet also spread across Windows computers through Step 7 project files. As mentioned, Step 7 is the software used to control PLCs, and Step 7 project files are located in a database. Any computer with this software installed was likely to have been used to input instructions into a PLCs that Stuxnet ultimately wanted access to. By infecting these project files, each time the project was opened from a different computer, Stuxnet would be able to infect that computer too.\textsuperscript{85}

Stuxnet was also capable of using peer-to-peer (P2P) methods to communicate with other infected computers within a LAN. The purpose of using these methods was to enable it to reach computers that were connected to a LAN but not the Internet. Also through P2P connections, information about the computers not connected to the Internet could be first sent to another computer on the LAN and then to the command and control servers via the Internet.\textsuperscript{86} This also allowed Stuxnet to update itself if these computers were running an older version of Stuxnet.\textsuperscript{87} Consequently, the use of P2P methods allowed the attackers to communicate with computers that Stuxnet had infected however, Stuxnet was also designed to function automatically without the need for external control.\textsuperscript{88}

Stuxnet therefore began by spreading across Windows computers. When Stuxnet reached a Windows computer, it would use different ways to inject itself into a process run by the computer depending on what security software was installed. It would determine which security software was installed and, if necessary, utilise one of its available zero-day

\begin{footnotesize}
\begin{enumerate}
\item Zetter (2014), p 90.
\end{enumerate}
\end{footnotesize}
exploits in this process. Once Stuxnet had injected itself onto a computer, it would run a series of checks to determine a range of things. In addition to which anti-virus software was installed, it would check whether a compatible version of Windows was installed, and depending on whether or not it had administrator rights, it would utilise one of its zero-day exploits to escalate its privileges. The aim was to obtain administrative privileges on the computer so that it could take any actions it wants. Stuxnet would also check to see whether the computer was already infected with a version of Stuxnet, and if so, whether it needed to be updated.

Once Stuxnet had installed itself onto a Windows computer and gathered information about the computer, it could contact the command and control servers and send information about the computer if (or when) it had Internet connectivity. This information included details about the ‘machine’s computer and domain names … as well as the internal IP address, the version of Windows it was running, and whether or not it had the targeted Siemens [Step 7] software installed on it.’ Based on information obtained from monitoring traffic to Stuxnet’s command and control servers, Symantec discovered that by 20 September 2010 there were approximately 100,000 infected host computers, and over 60,000 of these were in Iran. Connectivity to these servers also likely allowed Stuxnet to download and execute additional tools or updated versions of itself. The servers to which this information was sent were located in Malaysia and Denmark, and had been paid by stolen credit cards.

By using these techniques to spread across Windows computers, Stuxnet was ultimately able to spread to the specific PLCs it targeted. It targeted the S7-315 and S7-417 models of Siemens PLCs that were operated by Step 7 software. While the full version of Stuxnet contained the attack code for both of these models, the part of the code designed to attack S7-417 models was disabled meaning that only the code targeting S7-315 models was

active in the full version of Stuxnet.\textsuperscript{100} This was in contrast to Stuxnet 0.5 which only contained the S7-417 attack code and targeted the valves used to control the flow of UF\textsubscript{6} into the centrifuges.\textsuperscript{101} The attack code used in the full version of Stuxnet targeting S7-315 PLCs however, instead of targeting valves, targeted frequency converter drives. Specifically, it targeted S7-315 PLCs that were used to operate frequency converter drives that were manufactured by either Fararo Paya, an Iranian company, or Vacon, a Finnish company.\textsuperscript{102} Stuxnet searched for PLCs connected to specific hardware and checked, for example, the System Data Blocks (SDBs) of a PLC to determine how the PLC was configured and what hardware was connected to it.\textsuperscript{103} Therefore, it checked to see what the PLC was being used to control or operate. As part of this process, Stuxnet searched for specific part numbers found in frequency converter drives manufactured by either Fararo Paya or Vacon.\textsuperscript{104} Depending on the manufacturer of the frequency converter drive that the PLC was used to operate, Stuxnet could then use a slightly different infection sequence.\textsuperscript{105}

Another check that Stuxnet performed was to monitor these devices to ensure they were running between 807 Hz and 1210 Hz, as this was the frequency ranged it expected from its target.\textsuperscript{106} While it had not been confirmed that the facility at Natanz used the frequency converters manufactured by these companies, this frequency range corresponded to that at which the IR-1 centrifuges known to be used at the Natanz facility are operated.\textsuperscript{107} Additionally, there were values within the disabled part of the code targeting S7-417 PLCs that indicated IR-1 centrifuges were being targeted. An IR-1 centrifuge cascade contains 164 centrifuges, and the attack sequence of this part of the code was ‘grouped in six arrays of 164 each’ and this was believed to represent ‘six cascades, each with 164 centrifuges.’\textsuperscript{108} Therefore, this part of the code was searching for PLCs with 164 peripherals, and this corresponded with the number of centrifuges in each cascade.\textsuperscript{109} Given ‘that this array is identical to an IR-1 centrifuge cascade’ used at the Natanz facility, it has been described as

\begin{footnotesize}
\begin{enumerate}
\item McDonald et al (2013), p 9.
\item Falliere et al (2011), p 41.
\item Albright et al (2010), pp 3-4.
\item According to Falliere et al, ‘the code expects six groups of 164 peripherals’, see Falliere et al (2011), p 47. As mentioned, this part of the code was only active in Stuxnet 0.5 and it was disabled in the full version of Stuxnet.
\end{enumerate}
\end{footnotesize}
‘perhaps the strongest evidence’ that Stuxnet targeted the Natanz facility specifically.¹¹⁰ As such, these factors indicated that the PLCs that Stuxnet targeted were those used to control centrifuges used in the uranium enrichment process at the Natanz facility.

1.5 The Payload

Once Stuxnet found its targets, another part of its code would become active that would deliver the payload. According to Ralph Langer, an expert on industrial control systems, while Stuxnet’s propagation methods were complex, its payload was ‘rocket science’ in comparison.¹¹¹ Stuxnet’s payload was delivered in almost 27 day cycles. When Stuxnet infected a PLC that it targeted, it went through a five stage cycle of events. In the first state it monitored for data on the operation frequency of the frequency converter drives. Here it expected the drives to be operating between 807 Hz and 1210 Hz.¹¹² Once it had monitored a certain amount of data and recorded these events, usually after approximately 13 days, it transitioned to the second state. It then waited for two hours to transition to the third state. In both the third and fourth states, Stuxnet sent a burst of data containing instructions for the frequency converter drives.¹¹³ In the first cycle, Stuxnet adjusted the frequency of the frequency converter drive to 1410 Hz for 15 minutes and then back to 1064 Hz which is within the range of its normal operation.¹¹⁴ The rotation speed of the rotors inside the centrifuges to which this corresponded to has been described as ‘very close to the maximum speed the spinning aluminium IR-1 rotor can withstand mechanically.’¹¹⁵ This was the first cycle, and the second cycle took place approximately 27 days later. This cycle was similar to the first, but instead of increasing the frequency of the converter drives for 15 minutes, it lowered their speed by first setting the frequency to 2 Hz and then back to 1064 Hz over a 50 minute duration, and therefore slowed down the speed at which the rotor is rotated.¹¹⁶ As such, Stuxnet’s payload effectively sought to ‘sabotage[] the system by slowing down or

¹¹⁶ Falliere et al (2011), pp 42-43. The attack on S7-417 PLCs followed a similar process, but instead of altering the speed at which the rotors were spun, it opened and closed the valves used to feed UF₆ pinto the centrifuges. See McDonald et al (2013), pp 9-12.
speeding up the motor to different rates at different times.\textsuperscript{117} These cycles continued at approximately 27 day intervals.

While delivering its payload, Stuxnet also utilised what is known as a ‘man-in-the-middle’ attack. This term is used to describe ‘an unseen relay that intercepts, understands, alters, and retransmits a message for the purpose of deception.’\textsuperscript{118} Stuxnet used the data it gathered in the monitoring phase and played this back to the monitoring system of the PLCs to make it appear that the frequency converters were operating normally.\textsuperscript{119} It did so by replacing the file that is used by the Step 7 software in programming PLCs. As mentioned, PLCs function independently once they have been programmed.\textsuperscript{120} The file used by this software that is responsible for exchanges between the programming device (the Windows computer) and the PLC, is replaced by Stuxnet with a malicious version.\textsuperscript{121} Doing so allowed Stuxnet to monitor data sent to and retrieved from the PLC, alter the data, and mask the fact that the PLC is infected.\textsuperscript{122} Stuxnet also infected one of the Organisation Blocks (OB35) which was used by the PLC as an automatic safety mechanism capable of stopping any dangerous process being run by the PLC.\textsuperscript{123} During the third and fourth states of Stuxnet’s sabotage routine, the execution of this block was prevented.\textsuperscript{124} This is assumed to have prevented any shutdown that would normally occur during catastrophic events.\textsuperscript{125}

Therefore, Stuxnet adjusted the settings of the frequency converter drives responsible for the speed of the rotors within the centrifuges. When the rotation speed was raised, while it is likely that the 15 minute time period of the attack was not sufficient for the motor to actually reach the speed (equivalent to 1410 Hz) which would have guaranteed its destruction, the speed that it did reach in this time period was sufficient to disrupt the process and likely to also destroy the centrifuges.\textsuperscript{126} In contrast, when the rotation speed was lowered, this is likely to have degraded the uranium enrichment process meaning a lower amount of uranium was enriched.\textsuperscript{127} The combination of the two however, was likely done ‘with the

\textsuperscript{117} Falliere et al (2011), p 43.
\textsuperscript{118} Blahut (2014), p 511.
\textsuperscript{120} Falliere et al (2011), p 36.
\textsuperscript{121} Falliere et al (2011), p 36.
\textsuperscript{122} Falliere et al (2011), p 36.
\textsuperscript{124} Falliere et al (2011), p 49.
\textsuperscript{125} Falliere et al (2011), p 49.
\textsuperscript{126} Albright et al (2010), pp 4-5.
\textsuperscript{127} Zetter (2014), p 343.
intention of inducing excessive vibrations or distortions that would destroy the centrifuge.'128 As such, given its technical design, Stuxnet is understood to have been mainly intended to physically destroy the centrifuges and not simply, for instance, manipulate the ‘parameters of the centrifuge cascades so as to lower the production of low enriched uranium (LEU) on a sustained basis.’129

1.6 Iran’s Responses and the Effects of Stuxnet

Therefore, the design and purpose of Stuxnet are well understood from a technical perspective, and the 2011 and 2012 revelations by the New York Times confirm earlier suspicions that the US and Israel created Stuxnet. The effects of Stuxnet however – that is, whether it was responsible for the broken centrifuges – varies depending on whether Iranian or IAEA accounts are believed.

1.6.1 Iran’s responses

Iran has not confirmed that Stuxnet was the cause of broken centrifuges at Natanz however, Iranian officials have confirmed that some of their computers were infected by a computer virus. As will be shown below, particularly the statement made by Iran’s Vice President indicating that Iran had experienced issues with a computer virus in late 2009, indicates that Iranian computers were infected by a computer virus around the same time Stuxnet is believed to have been active. The timing of this infection, alongside IAEA reports indicating a decrease in the amount of active centrifuges around this time, suggests that Stuxnet was responsible for the broken centrifuges at the Natanz facility.

In September 2010 an Iranian official from the Ministry of Industry and Mines admitted that a computer ‘worm had infected more than 30,000 computers, including personal computers owned by employees of the nuclear power plant near Bushehr.’130 This worm was described as a form of ‘electronic warfare’ against Iran.131 Another official from

---

the Ministry of Communications and Information Technology however, maintained that ‘the effect and damage of this spy worm in government systems is not serious’ and that it had largely been halted. In November 2010, coinciding with IAEA reports that indicated Iran was having problems with its centrifuges at the Natanz facility, there were conflicting reports about whether Stuxnet was responsible for these problems. It was reported that, despite the above (September 2010) acknowledgements by Iranian officials of computers having been infected with a virus, Iran denied that this virus had ‘infected the operating systems at any nuclear site.’ However, according to reports later in November 2010, Iran’s President, Mahmoud Ahmadinejad, had stated that Iran’s enemies ‘had been successful in making problems for a limited number of our centrifuges, with software they had installed in electronic devices’. He also maintained that the source of the problems had been solved. When asked specifically about Stuxnet and whether it had been responsible, President Ahmadinejad’s response was one of silence. However, around this same time Iran’s Vice President, Ali Akbar Salehi, who is also the head of the Iranian Atomic Energy Organisation, maintained that ‘[o]ne year and several months ago, Westerners sent a virus to [our] country’s nuclear sites’, and that ‘with the help of God’ the virus was discovered and prevented from causing harm to Iran’s progress in the nuclear field. As will be discussed below, while the effects of the 2010 variants of Stuxnet remain unknown, the effects of the 2009 variant coincide particularly with the timeframe to which Iran’s Vice President’s statements refer to. Therefore, while Iran did not admit that Stuxnet specifically had managed to cause damage to its nuclear centrifuges, it did acknowledge that it had experienced issues with a computer virus. The timeframe referred to especially in the Vice President’s remarks corresponds to the time at which, according to IAEA reports, there was a decline in the number of operational centrifuges.

1.6.2 The IAEA’s reports

The IAEA releases quarterly reports on Iran’s implementation of NPT safeguards and UN Security Council resolutions. According to data compiled from these reports by ISIS (the

133 ‘Iran ‘briefly halted enrichment’, Al Jazeera, 23 November 2010.
136 When specifically asked whether Stuxnet was responsible, President Ahmadinejad responded by saying: ‘[t]he Iranian president's answer to this question is: silence. That's it.’ Erdbrink, ‘Ahmadinejad: Iran’s nuclear program hit by sabotage’, Washington Post, 29 November 2010.
137 Kessler, ‘Centrifuges in Iran were shut down, IAEA report says’, The Washington Post, 24 November 2010.
Institute for Science and International Security), between the November 2009 and February 2010 reports, the number of cascades enriching uranium decreased.\textsuperscript{138} As mentioned above, this timeframe refers specifically to when Stuxnet is known to have been active based on the timestamps in its log file, and the statement made by Iran’s Vice President regarding a virus sent by Westerners. According to the authors of the ISIS report, this means that between November 2009 and January 2010 one of the nuclear centrifuge cascade modules (A26) at the Natanz facility suffered problems requiring the decommission and replacement of about 1000 IR-1 centrifuges.'\textsuperscript{139} The authors of the ISIS report maintain that the module in question ‘suffered a major problem with at least 11 cascades directly affected.’\textsuperscript{140} This was evident in the sudden drop of centrifuge cascades under vacuum (a drop from 12 in the November 2009 report to 1 in the February 2010 report), and in the amount of cascades with disconnected centrifuges (a rise from 0 out of 18 in the November 2009 report to 11 out of 18 in the February 2010 report).\textsuperscript{141} By August 2010 the number of centrifuge cascades under vacuum and being fed with UF\textsubscript{6} had still not returned to their November 2009 levels.\textsuperscript{142}

In addition to this information from the IAEA’s reports corresponding with the statements by Iranian officials that their computer systems were infected with a virus, the IAEA’s video footage from the Natanz facility also shows that Iran was having problems there. The IAEA has surveillance cameras at the facility in order to monitor Iran’s compliance with NPT safeguards and UN Security Council resolutions. While these cameras only monitor the perimeter of the cascade areas and not the area itself,\textsuperscript{143} it has been reported that the footage shows that Iran had ‘dismantled more than 10 percent of the Natanz plant’s 9000 centrifuge machines used to enrich uranium.’\textsuperscript{144} This occurred in the six-month period following late 2009.\textsuperscript{145} IAEA officials who later examined the machines could not determine why they failed however, according to reports from European diplomats, the operators of the plant ‘worked frantically to replace each piece of equipment they removed’ in what was

\textsuperscript{138} Albright et al (2010), pp 2, 8.
\textsuperscript{139} Albright et al (2010), pp 1-2.
\textsuperscript{140} Albright et al (2010), p 2.
\textsuperscript{141} Albright et al (2010), pp 2, 8.
\textsuperscript{142} Albright et al (2010), pp 6, 8.
\textsuperscript{143} Albright et al (2011), p 3.
described as a determination to hide any drop in production from the IAEA safeguard reports.\textsuperscript{146}

\textit{1.6.3 Effects}

Therefore, based on this information it is generally believed that Stuxnet destroyed about 1000 of about 9000 IR-1 centrifuges at Natanz.\textsuperscript{147} This damage is understood to have been caused by the first (June 2009) variant of Stuxnet, as the exact effects of the 2010 variants (March 2010 and April 2010) remain unclear.\textsuperscript{148} Some, drawing on the technical design of Stuxnet, maintain it destroyed 984 centrifuges\textsuperscript{149} however, the IAEA has not provided such a specific number as it is unable to monitor every single cascade going in and out of the cascade area.\textsuperscript{150} In addition to these direct effects, particularly before Stuxnet was publicly revealed, it has been suggested that Iran was unlikely to have known the cause of the broken centrifuges.\textsuperscript{151} This in turn would have caused a degree of uncertainty and challenged its quality assurance program.\textsuperscript{152}

\textbf{Section 2: The Ontological Constraints of the Law}

As demonstrated in chapter 5, the Estonia incident highlighted the ontological constraints of the law as the incident is generally not considered a use of force particularly because the DDoS attacks against Estonia did not cause material damage. In contrast however, Stuxnet is generally considered to have constituted a use of force. As will be illustrated below, according to existing legal analyses of Stuxnet in relation to the use of force threshold, especially given that Stuxnet caused physical damage to centrifuges it is capable of being regarded as a use of force. Stuxnet therefore involved a form of violence that the law has the capacity to recognise. It is argued however, that as a result of the law’s ontological constraints it only provides a one-dimensional account of violence that does not adequately capture the non-material or informational harm that Stuxnet caused.

\begin{flushright}
\textsuperscript{148} See Zetter (2014), pp 354-357.
\textsuperscript{151} Albright et al (2011), p 1.
\end{flushright}
2.1 Stuxnet and the Use of Force Threshold

Stuxnet is widely considered in relation to questions surrounding when a cyber attack crosses the use of force threshold. The majority of authors, accepting that Stuxnet was the cause of the destruction of approximately 1000 centrifuges, maintain that it constituted a use of force particularly as it caused material damage to physical objects. For example, Gary Brown points to the fact that Stuxnet was ‘[i]ntentionally designed malware directed against a nation-state [and] resulted in the physical destruction of state-owned equipment. The centrifuges were destroyed as effectively as if someone had taken a hammer to them.’\(^{153}\) He therefore maintains that the incident violated the general prohibition on the use of force.\(^{154}\) Heather Harrison Dinniss also notes how, in contrast to the Estonia incident in which ‘[n]o loss of life, physical injury or destruction of property was suffered’ due to the cyber attacks, Stuxnet ‘purportedly resulted in significant destruction of property.’\(^{155}\) As a result, she takes the position that Stuxnet ‘would undoubtedly amount to a use of force.’\(^{156}\) David Fidler maintains that ‘a plausible argument can be made’ that Stuxnet constituted an illegal use of force.\(^{157}\) This is because its design reflected an intention ‘to cause physical damage – and the worm reportedly caused significant damage – to specific tangible objects in a particular location in one country: the uranium-enrichment centrifuges at Natanz, Iran.’\(^{158}\) Christopher DeLuca also suggests that Stuxnet would amount to a use of force because it involved the destruction of property – ‘parts of nuclear centrifuges in Iran were destroyed.’\(^{159}\) Andrew Moore argues that ‘[t]he destruction caused to the Iranian nuclear complex demonstrates that Stuxnet should be considered a use of force prohibited by Article 2(4).’\(^{160}\) Also, according to a number of authors including William Boothby and Michael Schmitt, Stuxnet qualifies as a use of force ‘[b]ecause the facilities suffered physical damage’.\(^{161}\) Finally, Marco Roscini, after noting that it is ‘virtually uncontested’ that a cyber attack causing (or which is

\(^{155}\) Dinniss (2012), p 81.
\(^{156}\) Dinniss (2012), p 82. She notes however, that ‘the scale and effects of the attack do not appear to have sufficient gravity to amount to an armed attack.’ Dinniss (2012), p 82.
\(^{157}\) Fidler (2011), p 57. He maintains that it could also be considered an armed attack, see Fidler (2011), p 57.
\(^{158}\) Fidler (2011), p 57.
\(^{159}\) DeLuca (2013), p 298.
\(^{160}\) Moore (2015), p 1. He maintains that under the traditional instrument based (that is ‘armed force’) definition of force, Stuxnet would not be considered a use of force. However, under the target, instrument, and effect based models that have been developed, it would be a use of force. Consequently, he writes that ‘[b]y targeting and destroying critical infrastructure in the Iranian nuclear complex, Stuxnet was a coercive use of the cyber instrument that had effects in the physical world.’ Moore (2015), p 22.
\(^{161}\) Boothby et al (2012), p 83.
reasonably likely to cause) physical damage to property constitutes a use of force, maintains that ‘the first known use of malicious software designed to produce material damage to physical property by attacking the SCADA [Supervisory Control and Data Acquisition] system of a NCI [National Critical Infrastructure] is Stuxnet.’ According to Roscini, it is evident that Stuxnet constituted a use of force as it caused the physical destruction of centrifuges. Therefore, for these authors, given that Stuxnet caused material damage to physical objects, it clearly constituted a use of force.

A number of authors also consider Stuxnet in relation to the Tallinn Manual criteria. In this context, most authors highlight the physical damage caused by Stuxnet in relation to the ‘severity’ criterion. For example, David Weissbrodt argues that ‘Stuxnet, at minimum, is considered to be a use of force.’ In relation to the severity criterion he notes that ‘the Stuxnet attack was severe because it caused physical harm to property. Stuxnet caused the centrifuges to speed up and slow down their rotation causing them to break.’

Priyanka Dev also examines the Stuxnet incident and argues that it constituted a use of force – particularly as it resulted in physical damage. He argues that the Tallinn Manual criteria support this conclusion, especially as there was severe harm to property. Andrew Foltz also notes in relation to the severity criterion that Stuxnet would be a use of force because it caused physical damage, even though the actual damage was minor and discrete. Charles Poché also examines Stuxnet through the Tallinn Manual criteria, suggesting that the incident would amount to a use of force. In relation Stuxnet’s severity he writes that: ‘acts causing physical harm cross the threshold as a use of force. Physical harm includes harm to property. The destruction of the centrifuges to necessitate their replacement meets this requirement.’

---

163 Some of these authors consider the Tallinn Manual criteria specifically, whereas others consider Schmitt’s criteria (which formed the basis for the Tallinn Manual criteria) before the Tallinn Manual was published. As also noted in chapter 5, for the sake of clarity, the term ‘Tallinn Manual criteria’ will be used instead of the term ‘Schmitt criteria’.
164 Weissbrodt (2013), p 376.
165 Weissbrodt (2013), p 376.
167 In examining the seven criteria, he maintains 1) there was severe harm to property; 2) the damage was immediate and did not allow Iranians to mitigate its consequences; 3) the damage was direct; 4) it was invasive as it completely controlled the computer systems, 5) the measurability was ‘medium’ as the consequences were identifiable but not quantifiable; 6) this criterion he argues was not applicable as there was neither any presumptive legitimacy nor illegitimacy; and 7) however, the degree of state involvement was unclear. See Dev (2015), pp 398-399.
168 Foltz (2012), p 44. He adds that it also set back Iran’s nuclear program for years and therefore impacted on its critical interests. Foltz (2012), p 44.
Finally, the authors of the Tallinn Manual also took the view that Stuxnet amounted to a use of force.\textsuperscript{171}

Given that Iran has not confirmed the destruction of centrifuges and the consequent degree of uncertainty around whether Stuxnet was responsible for their destruction, some commentators, while discussing Stuxnet and the law on the use of force, do not take a position as to whether or not Stuxnet in fact constituted a use of force. However, these authors’ analysis nonetheless reflects the importance of physical damage for determining whether a cyber attack crosses the use of force threshold. Katharina Ziółkowski for example falls within this group, arguing that whether Stuxnet constituted a use of force within the meaning of Article 2(4) depends on whether it ‘caused a non-trivial destruction of property.’\textsuperscript{172} Ultimately however, she does not take a position on this question, arguing that there is insufficient legal evidence to confirm physical damage.\textsuperscript{173} In light of this, she maintains that if indeed Stuxnet ‘did not cause any damage of physical nature, it appears not to reach the threshold of illegality pursuant to public international law and thus to be a ‘legal masterpiece’.\textsuperscript{174}

Similarly, Terry Gill argues that, even though the incident was downplayed by Iran, Stuxnet ‘may well have qualified as a use of force (short of an armed attack) in that it reportedly caused a degree of material damage and was intrusive enough to possibly be viewed as a use of force by some commentators’.\textsuperscript{175} Elsewhere, Terry Gill and Paul Ducheine note that unlike incidents such as Estonia which cannot be viewed as a use of force due to lack of ‘death, injury or significant long-term material damage to critical infrastructure on which the functioning of a State depends’, Stuxnet can be viewed otherwise given that it ‘reportedly caused a measure of physical damage to the centrifuges engaged in the enhancement of nuclear material.’\textsuperscript{176} As such, while these authors do not take a clear position on whether Stuxnet in fact constituted a use of force, they nonetheless highlight the importance of physical damage in making this determination. Finally, Russell Buchan also

\textsuperscript{171} Some in the Group of Experts also maintained it constituted an armed attack, see commentary to rules 10 and 13, Schmitt (2013b), pp 45, 58.
\textsuperscript{172} Ziółkowski (2012b), p 142.
\textsuperscript{173} Ziółkowski (2012b), p 140. Alternatively however, she does suggest Stuxnet could also constitute a use of force if it was significantly disruptive to Iran’s critical infrastructure comparable to the physical destruction of a facility or computer systems. Ziółkowski (2012b), p 142.
\textsuperscript{174} Ziółkowski (2012b), p 147.
\textsuperscript{175} Gill (2013), p 235.
\textsuperscript{176} Gill and Ducheine (2013), p 459.
questions the conflicting reports on whether or not there was in fact physical damage, and explicitly notes the difference this makes for the use of force analysis. He maintains that if Stuxnet simply ‘prevented the centrifuges from rotating at the correct speed’ meaning that uranium could not be enriched without the actual destruction of centrifuges, then Stuxnet ‘cannot be regarded as an unlawful use of force because no damage to physical property was caused.’ However, he argues that if the reports that Stuxnet did cause the physical destruction of centrifuges are correct, then ‘this would constitute the requisite physical damage in order for a violation of Article 2(4) to be established.’ Collectively, these analyses therefore highlight the need for known physical damage for a cyber attack to be considered a use of force, and that in relation to Stuxnet the primary obstacle for making this determination is the lack of sufficient certainty that it in fact caused the destruction of centrifuges.

As a result, unlike the Estonia incident which, according to the prevailing view, would not constitute a use of force especially because no physical destruction was caused, Stuxnet is more readily considered a use of force. As highlighted by the above accounts and those in relation to Estonia previously, this distinction is made largely on the existence of physical damage. For example, Foltz suggests (and this is something that Buchan also alluded to) that had Stuxnet only disrupted the operation of the uranium enrichment process and not destroyed centrifuges, it is unlikely it would have been considered a use of force. Hypothetically, if Stuxnet’s payload only involved the second sequence of the attack that sent instructions to the frequency converter drives to decrease the speed at which the rotors inside the centrifuges spun (and did not both decease and increase their speed as it did), this is likely to have only affected the amount of enriched uranium. This would therefore have undermined the ability of those centrifuges to enrich uranium, but potentially not have caused the destruction of the centrifuges. Yet there would have been little real difference in its

177 Buchan (2012), p 220.
179 Foltz asks: what if instead of damaging Iranian centrifuges Stuxnet achieved the same effects by causing the centrifuges to operate inefficiently or not at all? Except for severity, each of Schmitt’s factors would likely be evaluated the same. It is debatable, though, whether the international community would consider such an operation a prohibited use of force.
Foltz (2012), p 45.
180 As mentioned above, according to the ISIS report Stuxnet was designed to damage the centrifuges and not to manipulate the ‘parameters of the centrifuge cascades so as to lower the production of low enriched uranium (LEU) on a sustained basis.’ See Albright et al (2011), p 1.
overall effect in undermining Iran’s ability to properly enrich uranium with those centrifuges, even if the centrifuges remained physically intact.

However, as is evident in the above analyses of Stuxnet in light of the use of force, had this been the case and therefore that Stuxnet only disrupted the uranium enrichment process but did not cause physical damage to centrifuges, it is unlikely that it would have so widely been considered a use of force. Instead, it is likely to have been considered to fall below the use of force threshold and amounted to a breach of the non-intervention principle alone. As highlighted in the context of the Estonia incident however, the artificial distinction essentially between cyber attacks with and without material effects highlights the law’s ontologically constrained view of violence. As Stuxnet caused physical damage to centrifuges and thus constituted a cyber attack with material effects, the law has the capacity to recognise it as a form of violence. It is argued however, that as these legal analyses show, the law offers a one-dimensional account of violence in the sense that it lacks depth because the focus is mainly on the material effects of Stuxnet. Unlike the Estonia incident which was not captured by the law’s depiction of violence due to its ontological constraints, while the law has the capacity to recognise Stuxnet as a form of violence, it only offers a one-dimensional account that does not adequately capture the informational harm that Stuxnet caused. Consequently, as the next section argues, an informational approach offers a means to appreciate the informational and physical forms of violence that the Iranian entity was subject to and hence provides a deeper account of violence.

Section 3: An Informational Approach

The cyber attacks against Estonia examined in chapter 5 were depicted as a form of informational violence causing entropy. By disrupting the functioning of Estonia’s government and civil society, the attacks constituted a form of informational violence that caused increased entropy within the Estonian entity. On the other hand, the harm caused by Stuxnet involved the destruction of physical objects in the real world. As illustrated above, it can hence more easily be regarded as a form of violence capable of being recognised by the law. However, it is argued that this emphasis mainly on Stuxnet’s material effects does not

---

181 Gill for example, while not taking a definitive position on whether Stuxnet constituted a use of force, nonetheless maintains that Stuxnet definitely qualified as an ‘intervention’ given that it involved coercive means to prevent a state from ‘pursuing a particular course of action’. See Gill (2013), p 235.
adequately account for the numerous ways in which it caused non-material harm. In other words, the law only provides a one-dimensional account of violence due to its ontological constraints. As such, this section provides an informational analysis of Stuxnet to argue that an informational approach offers a means to appreciate both the informational and physical forms of harm that Stuxnet caused, instead of primarily focusing on its material effects that dominate existing legal analyses of the incident. Therefore, it is argued that Stuxnet was not simply an example of physical violence causing entropy, but instead can be seen as combination of physical and informational forms of violence causing entropy within the Natanz system and in the Iranian entity’s region of the infosphere. Accordingly, like the informational analysis of the Estonia incident in chapter 5, this section will first describe the Iranian entity as an information system with a responsibility to care for and protect its region of the infosphere. It will then consider the Stuxnet attack as a form of both physical and informational violence causing entropy. It is argued that in contrast to the law’s one-dimensional account of violence, an informational approach offers a means to appreciate the depth of violence that the Iranian entity was subject to.

3.1 The Iranian Entity and the Natanz System

In contrast to the Estonian entity, the Iranian entity is a less developed information society. For example, within its region of the infosphere only approximately 44% of households have Internet access,\(^{182}\) there is a smaller but growing number of Internet users at under 40% of the population,\(^{183}\) and the levels of access to ICTs, the level of development of its ICT infrastructure and level of use of ICTs across society are slightly below the global average.\(^{184}\) Iran has also begun to develop its e-government services,\(^{185}\) though a developing ICT infrastructure means Iran is also faced with technological barriers in this effort.\(^{186}\)

---


\(^{184}\) In 2015 Iran’s IDI was 3.48 with the global average of 5.03, ranking it 91\(^{11}\) in the world. See International Telecommunication Union (2015), pp 44-46. As mentioned in chapter 5, the ITU’s ‘ICT Development Index’ (IDI) combines various indicators ‘to monitor and compare developments in information and communication technology (ICT) between countries and over time.’ International Telecommunication Union (2015), p 39. These indicators include the ICT readiness of the country (its level of networked infrastructure and access to ICTs), the ICT intensity (the level of ICT use in society), and the ICT impact (the outcomes of efficient and effective ICT use, or the ICT skills). International Telecommunication Union (2015), pp 39-41.

\(^{185}\) For an overview of the laws and policies since 2000 relating to Iran’s development of e-government, see Bigdeli and de Cesare (2011), pp 308-309. For an overview of the history of the implementation of ICTs into Iran’s administrative and government communications, see Sharifi and Zarei (2004), pp 605-606.

Nonetheless the Iranian entity is a dynamic entity, as its informational substance continuously changes over time with various flows of information moving in and out of it.

Like the Estonian entity as an information system, the Iranian entity has systematic features. It is autonomous as it has a degree of independence from its environment and from other entities. Despite structural reconfigurations in 1979 when it transitioned from a monarchy to a republic, the Iranian entity has political independence and continues to operate as an independent state entity separate from other state entities. It is also capable of interacting with other entities, including other state entities in the physical proximity of its region of the infosphere, and international organisations such as the UN and the IAEA. It is an adaptable entity capable of changing its policies and strategies depending on the information it receives from its environment. As a state entity, its inherent purpose is to care for and protect its region of the infosphere, including the various entities and processes, such as its nuclear program, within this region.

The form or pattern of the Iranian entity is also evident in its structural configuration. Its information structures are, for instance, evident in the organisation of its executive, legislative and judicial institutions. Its executive includes the offices of the Supreme Leader and President, and the Council of Ministers (cabinet). The Islamic Consultative Assembly in turn performs the legislative functions, whereas the Supreme Courts and lower courts are organised and structured to perform judicial functions. The overall structural configuration of these entities and their basic tasks and functions are in turn set out in the Constitution of the Islamic Republic of Iran which provides the overarching protocol governing the interactions of these entities, and embeds a particular value system into the Iranian entity. Among other key internal protocols governing the interactions of these entities and their relationships to the environments within the Iranian entity’s region of the infosphere are public and administrative law, and environmental law. These structures and protocols delineate the Iranian entity from other state entities, and give it a degree of internal coherence.

Given the Iranian entity’s nuclear program, an important external protocol governing the interactions between the Iranian entity and the majority of other state entities is the NPT.

---

For example, Homa Katouzian describes Iran’s 1979 constitution as having both theocratic and secular/democratic elements, see Katouzian (2009), pp 335-337. Similarly, Said Arjomand describes it as an ‘ideological constitution’ as all laws have to be in accordance with Islamic standards, see Arjomand (2013), pp 31-32.
The NPT regime’s protocols are aimed at regulating the proliferation of nuclear weapons, promoting the peaceful use of nuclear energy, and disarmament of nuclear weapons stockpiles. In effect the NPT protocols are designed to restrict the spread and development of nuclear technologies given the capability of these technologies to cause the large scale destruction of information entities and parts of the infosphere. As an autonomous entity, Iran has since 1968 agreed to operate according to the NPT protocols. The Iranian entity is also bound by the safeguard agreements pursuant to which it has authorised the IAEA to monitor its nuclear program. However, the international system considers the Iranian entity’s nuclear program to be for non-peaceful purposes and contrary to the operational limitations of state entities provided by the NPT protocols. The Iranian entity’s nuclear program, including the enrichment facility at Natanz which is part of this program, is therefore considered a potentially hostile and malicious process within the Iranian entity’s region of the infosphere. This is because it is operated contrary to the external protocols governing the interactions between the Iranian entity and other state entities within the international system.

This is illustrated by various decisions made by the entity responsible for maintaining international peace and security within the infosphere – the UN Security Council – the decisions of which constitute protocols according to which all state entities are bound in their interactions. The UN Security Council has in several of its decisions recognised that the Iranian entity’s nuclear program is a process in contravention of the NPT protocols. As a result it has imposed restrictions on various information flows in and out of the Iranian entity. For example, in 2006 the UN Security Council passed a resolution recognising the potential military dimension to Iran’s nuclear program contrary to the NPT, and demanded that Iran suspends ‘all enrichment-related and reprocessing activities’. The same year the UN Security Council, ‘mindful of its primary responsibility under the Charter of the United Nations for the maintenance of international peace and Security,’ imposed sanctions on Iran. It limited the ability of all state entities to supply, sell or transfer any ‘items, materials, equipment, goods and technology which could contribute to Iran’s enrichment-related, reprocessing or heavy water-related activities, or to the development of nuclear

---

weapon delivery systems’. This resolution also required other state entities to inform the sanctions committee about the movement of any individuals within their territories ‘who are engaged in, directly associated with or providing support for Iran’s proliferation sensitive nuclear activities or for the development of nuclear weapon delivery systems’. Further, the UN Security Council decided that all states shall freeze any funds within their territories ‘owned or controlled by the persons or entities’ associated with or supporting Iran’s nuclear program. Numerous other resolutions relating to Iran’s nuclear program have also been passed since 2006. For example, in 2008 the UN Security Council decided that other state entities should not simply inform the sanctions committee about the movement of designated persons associated with Iran’s nuclear program, but also ‘take the necessary measures to prevent the entry into or transit through their territories’. Therefore, the UN Security Council, as the entity responsible for international peace and security within the infosphere, has deemed Iran’s nuclear program as a malicious process given its operation contrary to the NPT protocols. As a result of this and in an effort to ensure the Iranian entity ends this malicious process and recommences operation according to the NPT protocols, the UN Security Council has restricted various flows of information (ranging from goods, services and technologies, to humans and financial activities) in and out of the Iranian entity’s region of the infosphere.

As part of Iran’s nuclear program, the Natanz facility as a process can be considered a sub-system of the Iranian entity which is also located within its region of the infosphere. The Iranian entity continues to operate the Natanz system and its nuclear program generally, and adapt its operation to the external protocols restricting information flows in and out of its region of the infosphere, maintaining its autonomy and adaptability as an entity. Maintaining the operation of this process enables it to provide energy and security to entities within its region of the infosphere, and it is regarded by Iran as essential in maintaining its ability to

194 See, for example, Dupont (2012), pp 303-306.
care for and protect the wellbeing of its region of the infosphere.\footnote{According to Gawdat Bahgat, Iran’s nuclear policy is driven by the dynamics of its security environment, domestic political and economic concerns, and its national pride in developing a self-sufficient nuclear program. See Bahgat (2006), pp 313-324.} This is despite the officials responsible for the operation of Iranian entity knowing that the continued operation of this process is contrary to the external protocols according to which the Iranian entity has agreed to operate. Nonetheless, its internal protocols continue to authorise the operation of this process which the international system regards as malicious. As such, given its responsibility to care for and protect all entities within its region of the infosphere, the Iranian entity has also sought to protect the integrity of the Natanz system as a component of its nuclear program. For example, to protect the integrity of the Natanz system, it has been disconnected from digital flows of information from the rest of the infosphere as a means to protect it from potential threats capable of causing increases in entropy.

3.2 Stuxnet and Entropy

Stuxnet was a technically sophisticated piece of malicious software and demonstrated that its designers had extensive knowledge of the ‘structure and daily rhythms’\footnote{Sanger, ‘Obama Order Sped Up Wave Of Cyberattacks Against Iran’, The New York Times, 1 June 2012.} of the Natanz system. It was specifically designed to undermine the operation of Iran’s nuclear program by causing increased entropy within the Natanz system. However, the degrees of entropy produced by various parts of Stuxnet varied, ranging from undermining the integrity of computers and exploiting the communication protocols between computers, to delivering a payload causing physical damage to approximately 1000 centrifuges. As this section will show, Stuxnet can be seen as inflicting both informational and physical forms of violence causing increases in entropy within the Natanz system.

3.2.1 Propagation methods

The original infection method and propagation methods used by Stuxnet allowing the introduction and spread of Stuxnet into and throughout the Iranian entity resulted in various degrees of increases in entropy. While it remains unknown exactly how and when Stuxnet 0.5 was introduced into Natanz, from the information obtained from Stuxnet’s log file, the June 2009, March 2010, and April 2010 variants first infected the computers of five separate
companies. Through these computers Stuxnet then spread into the Natanz system. The initial infection of the first computers within these companies can only be considered a very minor increase in entropy. However, over time approximately 12,000 computers within these corporate entities were infected leading to a larger increase in entropy given the total amount of infected computer systems. Stuxnet ultimately spread and infected over 100,000 computers around the world which in turn can be regarded as a more significant increase in entropy. Over 60,000 of these were located within the Iranian entity’s region of the infosphere. While these computers continued to operate normally, their integrity was compromised. Stuxnet would for example check which anti-virus software was installed on a computer and choose the most appropriate injection process into that computer, and if necessary also utilise one of its zero-day vulnerabilities to inject itself into an active process run by the computer. Also without the authorisation of the legitimate users, Stuxnet granted itself administrator rights through the exploitation of zero-day vulnerabilities. It was therefore capable of bypassing the security mechanisms of each computer system which were designed to protect these entities from threats capable of causing increases in entropy.

Further, given that Stuxnet had administrator rights on each computer, it was capable of taking any action it wanted. While it only delivered its payload to very specific computer configurations and only sent basic information about the other computers it infected to the command and control servers, it is understood to have had the ability to download additional features from these servers. While it did not disrupt the operation of these computers, it had undermined their integrity and was able to communicate with other computers infected by Stuxnet and the command and control servers, update itself, and even potentially obtain additional features. As such, in addition to the entropy caused in undermining the integrity of these computers in the above ways, Stuxnet also had a further potential to cause more increases in entropy in the over 100,000 entities it had infected.

The computers used within the Natanz system to program the PLCs (and the PLCs themselves) were specifically configured so as to protect them from entropy and keep them secure from potential threats that could come through the Internet. Through an air-gap

---

limiting the flows of digital information into these computers, the Iranian entity sought to protect the integrity of these computers and the processes they were used to operate within the Natanz system. As such, the Natanz system’s interactions with other entities, even within the Iranian entity’s region of the infosphere, were limited to those with physical access to it. Consequently, the attackers exploited other information flows into the Natanz system in order to infect it with Stuxnet. These included, for example, USB drives and programmers and engineers with physical access to the Natanz system. Stuxnet was able to copy itself onto USB drives using a driver file which was signed with a stolen digital certificate meaning it would be trusted by the system as a safe file. One of the methods it used in this process of spreading to and from USB drives was the exploitation of a zero-day vulnerability in .LNK files. This allowed Stuxnet to execute automatically whenever the USB drive containing Stuxnet was inserted and the folder displaying the contents of the USB was viewed. Stuxnet was able to spread to subsequent computers into which the USB drive was inserted and ultimately infect computers used within the Natanz system. In order to mask that these entities were the source of Stuxnet’s infection, Stuxnet was able to hide its files on the USB drives and it also deleted itself from them once it had been used to infect three computers. As the main propagation method used, by spreading to and from USB drives Stuxnet was able to spread across the computers of humans working for corporate entities involved with Iran’s nuclear program and consequently obtain access to the secured Natanz system. Therefore, while the Natanz system was disconnected from the Internet, Stuxnet exploited other information flows into the Natanz system. In this context it produced entropy by undermining the integrity of the Natanz system, and by doing so it also undermined the Iranian entity’s ability to care for and protect the Natanz system from entropy.

In addition to the entropy caused by Stuxnet in the process of undermining the integrity of the Natanz system, the various other propagation methods used to further spread and reach the PLCs also caused increases in entropy. In addition to USB drives, the propagation methods also made use of P2P connectivity and LANs, and involved the exploitation of information exchanges between entities. For example, by exploiting the print-spooler vulnerability of computers connected to a shared printed through a LAN, Stuxnet enabled unauthorised information exchanges between these computers and used these
exchanges to spread.\textsuperscript{207} Also, by infecting Step 7 project files located in a database, Stuxnet was able to spread to computers using the Step 7 software and to those computers used to configure PLCs.\textsuperscript{208} Therefore, Stuxnet caused increases in entropy by undermining and degrading the integrity of the normal information exchange processes between computers sharing a printer on a LAN, and between computers using Step 7 software to access project files. Finally, by exploiting P2P connectivity within a LAN, Stuxnet enabled information exchanges to and from computers that had been configured to be secure and disconnected from the Internet.\textsuperscript{209} This way Stuxnet could communicate with computers not connected to the Internet and relay information about these computers to the command and control servers. In addition to causing increases in entropy by undermining the integrity of these computers, Stuxnet also caused increases in entropy by undermining the non-networked configuration of these computers. Through these propagation methods collectively, Stuxnet was able to undermine the integrity of these computers and their interactions, and it ultimately undermined the integrity of the PLCs it reached using these methods. Doing so caused increases in entropy within the infected computer systems and within the Natanz system as a whole.

\textit{3.2.2 Man-in-the-middle}

Besides the entropy produced by Stuxnet’s propagation methods, the man-in-the-middle attack also produced increases in entropy. Stuxnet replaced the legitimate library file that is used by the Step 7 software to communicate with PLCs with its own version.\textsuperscript{210} This allowed Stuxnet to monitor the data sent to and from the PLC, to send its own data or replace existing data being sent to and from the PLC, and hide the fact that the PLC was infected.\textsuperscript{211} As a result, Stuxnet was capable of intercepting and manipulating the data that was communicated between the computer operating Step 7 software and the PLC used to configure the operation of the centrifuge cascades. Using the data that Stuxnet had obtained during the monitoring phase, the man-in-the-middle attack allowed it to feed data showing the normal operation of the frequency controllers to the operators of the Natanz system and prevented them from

\textsuperscript{208} Falliere et al (2011), pp 25, 33.
\textsuperscript{210} Stuxnet replaced the original s7otbxdx.dll file with its own version, and renamed the original as s7otbxsx. See Falliere et al (2011), pp 37-38.
\textsuperscript{211} Falliere et al (2011), p 36.
receiving ‘the anomalous operating frequency data’\textsuperscript{212} that would have otherwise been sent while it delivered its payload. This undermined the integrity of the information that was being relayed from the Step 7 software to the PLC used to operate centrifuge machines, and the information relayed to and relied upon by the human operators of the Natanz system. Also by replacing the library file with a malicious version, Stuxnet undermined the integrity of relationship between the Step 7 software and the PLC it was used to configure. By doing so and undermining the integrity of this information exchange process, Stuxnet caused further increases in entropy. Additionally, by infecting the OB35 data block used by the PLC as a safety mechanism for when it is faced with catastrophic events, Stuxnet prevented the operation of digital alarm systems that would have otherwise been triggered. Stuxnet prevented the PLC from executing this data block during the third and fourth states of its sabotage routine, and this is understood to have prevented the system’s automatic shutdown that would normally occur during catastrophic events.\textsuperscript{213} Stuxnet therefore disabled a protective function that would have otherwise indicated that a component of the Natanz system was threatened by an entity capable of causing increased entropy.

### 3.2.3 Payload

In addition to the various degrees of entropy caused by Stuxnet’s propagation methods and its man-in-the-middle attack, the most significant amount of entropy was caused by its payload. Among the necessary conditions required by Stuxnet before it delivered its payload was that it had found a S7-315 PLC used to operate a frequency converter drive manufactured by either Fararo Paya or Vacon\textsuperscript{214} which was operating at between 807 Hz and 1210 Hz.\textsuperscript{215} Then during the third and fourth states of the 27 day attack cycle Stuxnet sent bursts of data containing instructions determining the operation of the frequency converter drives used to control the rotation speed of the centrifuges.\textsuperscript{216} In the first cycle, Stuxnet adjusted the frequency of the frequency converter drive to 1410 Hz for 15 minutes and then back to 1064 Hz.\textsuperscript{217} This resulted in an increase in the rotation speed of the centrifuge that is believed to be sufficient to both disrupt the enrichment process and destroy the centrifuge.\textsuperscript{218} Approximately

\textsuperscript{212} Falliere et al (2011), p 49.
\textsuperscript{213} Falliere et al (2011), p 49.
\textsuperscript{215} Falliere et al (2011), p 41.
\textsuperscript{216} Falliere et al (2011), pp 42-43.
\textsuperscript{218} Albright et al (2010), pp 4-5.
27 days later in the third and fourth states of the second cycle, Stuxnet sent another burst of data adjusting the frequency to 2 Hz for 50 minutes then back to 1064 Hz meaning the centrifuge rotors were slowed down.\textsuperscript{219} This is believed to have degraded the uranium enrichment process meaning a lower amount of uranium was enriched.\textsuperscript{220} As such, Stuxnet altered the information sent from the PLC to the frequency converter drives, and as the normal operation frequency of these devices is between 807 Hz and 1210 Hz,\textsuperscript{221} it corrupted the normal properties of these entities when used for uranium enrichment. The combined result of the two cycles demonstrated that Stuxnet was intended to induce ‘excessive vibrations or distortions’ capable of physically damaging the centrifuge.\textsuperscript{222} Instead of simply instructing the frequency converter drives or the PLC to shut down for example, Stuxnet’s payload involved a more subtle adjustment of the settings of these devices for 15 and 50 minute periods at approximately 27 day intervals. In addition to the entropy caused by the corruption of the frequency converter drives and the consequent disruption of the normal operation of the centrifuges, Stuxnet is believed to have caused material damage to approximately 1000 IR-1 centrifuges. Therefore, its payload resulted in a significant degree of increased entropy within the Natanz system. This was also evident from the IAEA’s reports demonstrating that there was a sudden drop in the number of centrifuges under vacuum and a rise in the number of cascades with disconnected centrifuges,\textsuperscript{223} as well as video footage showing that a similar number of centrifuges were dismantled.\textsuperscript{224} In effect, these reports indicated that the Natanz system was not operating normally and that, given the timing, Stuxnet was the likely cause of these increases in entropy.

### 3.2.4 The Iranian entity’s responses

The exact measures taken by the Iranian entity’s officials in response to Stuxnet are unknown however, statements by some of its officials about the incident reflect a recognition that the Iranian entity was under threat. These statements effectively show that the Iranian entity’s capacity to care for and protect the entities within its region of the infosphere was undermined by Stuxnet and the increases in entropy it is believed to have caused. For

\textsuperscript{219} Falliere et al (2011), pp 42–43.
\textsuperscript{220} Zetter (2014), p 343.
\textsuperscript{221} Falliere et al (2011), p 43.
\textsuperscript{222} Albright et al (2010), p 6.
\textsuperscript{223} Albright et al (2010), pp 2, 8.
example, in September 2010 an official from the Ministry of Industry and Mines admitted that 30,000 computers had been infected by a hostile entity including the computers of those working at the nuclear facility near Bushehr.\textsuperscript{225} Similarly, in November 2010 Iran’s President acknowledged that Iran’s enemies had been successful in creating problems for its centrifuges using software even though he maintained that the problem had been solved.\textsuperscript{226} Finally, Iran’s Vice President too acknowledged that a hostile entity had infected its nuclear program but that it was ‘discovered and prevented from causing harm’ to the operation of this program.\textsuperscript{227} These senior officials within the Iranian entity explicitly recognised the hostile nature of Stuxnet and its ability to cause increased entropy within its region of the infosphere. These statements also demonstrate that the Iranian entity was taking measures to prevent Stuxnet from causing further entropy within its nuclear program so that it could continue the operation of this process. As an entity responsible for the care and protection of entities within its region of the infosphere, the Iranian entity recognised that Stuxnet was a hostile entity capable of causing increases in entropy within the Natanz system and undermining its nuclear program.

Therefore, the Iranian entity, like the Estonian entity, is a dynamic entity constituted by various information structures and which operates according a range of protocols. With its nuclear program deemed a malicious process by the external protocols of the NPT regime, the international system has restricted a range of information flows in and out of this entity. As an autonomous entity responsible for the care and protection of its region of the infosphere, the Iranian entity continues to operate its nuclear program contrary to the NPT protocols. The Natanz system is a key component of this program within the Iranian entity’s region of the infosphere and was intentionally infected with Stuxnet by other state entities (the US and Israel). Stuxnet caused a range of increases in entropy within the Natanz system, including undermining the integrity of computers and delivering a payload which caused material damage to approximately 1000 centrifuges. Given its various features, Stuxnet can be seen inflicting both informational and physical forms of violence causing entropy within the Natanz system.

\textsuperscript{227} Kessler, ‘Centrifuges in Iran were shut down, IAEA report says’, \textit{The Washington Post}, 24 November 2010.
As demonstrated above in section two, existing legal analyses of Stuxnet and the use of force stress the importance of the material damage to the centrifuges caused by Stuxnet. Unlike the DDoS attacks against Estonia which were primarily disruptive and generally are not considered to have constituted a use of force (and instead only a breach of the non-intervention principle), particularly because Stuxnet did cause material damage it is more widely considered to have crossed the use of force threshold. This means that Stuxnet can be more easily recognised by the law as a form of violence when compared to the attacks against Estonia – primarily based on the fact that it caused (or is at least believed to have caused) material damage to approximately 1000 centrifuges. As Ziolkowski noted above, if Stuxnet had merely disrupted the operation of the centrifuges without causing material damage, it could be described as a ‘legal masterpiece’. In other words if this was the case, Stuxnet would have only constituted a form of informational violence that is not adequately captured by the law. Without causing material damage, Stuxnet is likely to have fallen outside the scope of the use of force principle and would have instead been depicted as a potential breach of the non-intervention principle. This is due to the tendency, as demonstrated particularly in chapter 4, to cast non-material cyber attacks into the ambit of the non-intervention and into the periphery of the use of force doctrine. Such cyber attacks are cast outside the conception of violence reflected in the law and instead represented as a form of non-violence.

Therefore, it is argued that while the law’s ontological constraints do not prevent the law from recognising Stuxnet as a form of violence, due to these constraints it only provides a one-dimensional account of violence that does not adequately capture the informational harm that Stuxnet caused. Essentially the law does not sufficiently account for the ways in which the functioning of state entities can be undermined also through non-material harm or informational violence. Instead, the law remains premised on the view of the state as a static territorial entity and on the view of violence that requires material damage or destruction or physical property, or injury or death to human beings. However, because of the new ways in which increasingly ICT dependent states can be harmed, this is a one-dimensional account of violence. It does not adequately account for the informational violence that Stuxnet caused.

Ziolkowski (2012b), p 147. Similarly, Foltz suggests that it is unlikely to have been considered a use of force by the international community, see Foltz (2012), p 45. This point is also made by Buchan, see Buchan (2012), p 220.
Stuxnet spread through the computers of corporate entities using stolen digital signatures and it exploited vulnerabilities in commercial software. It effectively masked itself as a trusted information process in order to spread through commercial software installed on the computers of private entities, to obtain access and undermine the integrity of the secure systems within the Natanz enrichment facility. Consequently, Stuxnet exploited and undermined the integrity of the interactions between a range of public and private entities and processes, causing various forms of non-material harm and also material damage to centrifuges. As such, the violence it involved was more than simply the material damage caused to centrifuges.

By viewing the state entity as a dynamic entity or information system, the essence and functioning of which can be undermined by cyber attacks with material and non-material effects causing entropy, both a broader spectrum of violence can be recognised and also a deeper account of violence can be considered. As demonstrated above, an informational analysis of the various ways in which Stuxnet spread, compromised computers and ultimately adjusted the rotation speed of nuclear centrifuges, provides a more in-depth account of the harm caused by Stuxnet and how it did so. The entropy caused by the payload resulting in physical damage to centrifuges, while significant in degree, was only part of the overall increases in entropy that Stuxnet caused. Accordingly, instead of focusing purely on the material effects caused by Stuxnet’s payload, more emphasis can be given to the various ways in which it corrupted the properties of over 60,000 entities within the Iranian entity’s region of the infosphere, how it undermined the integrity of the Natanz system, as well as how it disrupted and damaged the operation of centrifuges used in the enrichment process. Therefore, an informational approach provides a means to overcome the law’s ontological constraints meaning the law can be updated to recognise a broader spectrum of violence, and this also enables it to account for a deeper understanding of violence. This emphasises both the material and non-material ways in which Stuxnet’s various parts sought to undermine the operation of the Iranian entity’s nuclear program. As such, Stuxnet can be seen as a form of both informational and physical violence causing entropy within the Iranian entity and to the Natanz system specifically.

Finally, an important consideration in relation to the overall harm caused by Stuxnet is its wider context and whether it contributed to the wellbeing of the global infosphere. Stuxnet was essentially a malicious entity designed to undermine the operation of another
entity, namely the uranium enrichment process run by the Natanz system as part of Iran’s nuclear program. However, the international system had, through various UN Security Council resolutions, deemed the Iranian nuclear process contrary to the NPT protocols. As such, within the international system as a whole, the Natanz system was considered a malicious entity given its potential to contribute to more widespread and significant increases in global entropy through the unauthorised proliferation of nuclear weapons technologies. In this context, while not expressly authorised by the international system, Stuxnet can be viewed as an effort by other state entities to disrupt the operation of the Natanz system and prevent potential increases in global entropy. Therefore, despite the fact that Stuxnet itself was a malicious entity that caused increases in entropy particularly within the Iranian entity’s region of the infosphere, it sought to disrupt the operation of a more malicious entity that had the potential to cause more significant increases in global entropy. Accordingly, Stuxnet can be seen as designed to promote the Iranian entity’s compliance with the NPT protocols and promote the wellbeing of the infosphere as a whole by removing potential sources of entropy.
Chapter 7: Conclusion

In 1996 Krystyna Gorniak-Kocikowska predicted that, given the global nature of cyberspace and the nature of the ‘computer revolution,’

the ethic of the future will have a global character. It will be global in a spatial sense, since it will encompass the entire Globe. It will also be global in the sense that it will address the totality of human actions and relations.¹

This is in contrast to the ethical theories of Immanuel Kant and Jeremy Bentham that, she argues, despite their claims to universalism are the manifestation and culmination of a particular European Enlightenment.² Also in 1996, writing in relation to the impact of ICTs on public international law and warfare, Sean Kanuck argued that:

Just as territorial boundaries and natural resources formed the theoretical foundation for an international legal paradigm in an age of geopolitical borders, so too must a conceptual framework based on information undergird the legal institutions of the twenty-first century.³

He maintained that the basis for this new system must be interactions and not physical territory.⁴

This thesis has answered the call for a ‘new international legal paradigm’ for the information age that moves beyond ‘territorial boundaries and natural resources’. Floridi’s information ethics offers a conceptual framework based on information and it is concerned with the interactions of all information entities. As such, it provides an ‘ethic of the future’ that is designed to ‘address the totality of human actions and relations’ in the information age.

This chapter begins with an overview of this thesis and how information ethics was used to develop an informational approach to international law on the use of force in relation to cyber attacks. Following this, it considers the contribution of this thesis to information ethics as a field. It then briefly examines the relationship between law and informational

³ Kanuck (1996), p 274.
violence, and how the law on the use of force can be reformed. Finally, and to conclude this thesis, this chapter explores both the wider implications of an informational approach for international law, and potential sites for future research.

**Thesis Overview**

Floridi’s information ethics is among efforts to provide a more universal ethics that is concerned with the impact of the interactions of all entities on the infosphere. As demonstrated in chapter 2, it is grounded in a philosophy of information and it adopts an informational view of the world, placing the ability to interact as central to what constitutes being.\(^5\) It offers an environmental ethics concerned with the wellbeing of all of the entities and environments that make up the global infosphere. In doing so, it extends its ethical concern beyond anthropocentric or even ‘biocentric’ theories towards an ‘ontocentric’ one.\(^6\) The universal or global basis stems in part from the idea that the ethical dimensions of information and ICTs concern everyone.\(^7\) Floridi’s information ethics in particular seeks to be universal in the sense of being all inclusive, because, given that all entities can be seen as information entities, its ethical framework seeks to address issues affecting all of them.\(^8\)

Therefore, information ethics incorporates not only the digital world of cyberspace, the world’s natural environment, or humans and other sentient beings as the focus of its ethical concern, but instead all of these entities, environments, and the global infosphere that they constitute. Accordingly, information ethics provides an ethic with a truly global character that encompasses the totality of interactions and relations between information entities.

In this thesis information ethics was drawn on essentially to consider the harm that cyber attacks can cause to the state. This was driven by a sense that state activities in and

---

\(^5\) According to Floridi:
the criterion for existence—what it means for something to be completely and ultimately real—is also changing. Oversimplifying, ancient and medieval philosophers thought that only that which is immutable, that is, God, could be said to exist fully. Anything that changes, such as an animal, moves from non-existence (there was no animal) to existence the animal was born) back to non-existence (the animal is dead). Modern philosophers preferred to associate existence to the possibility of being subject to perception. The most empirically minded insisted on something being perceivable through the five senses in order to qualify as existing. Today, immutability and perceivability have been joined by interactability. Our philosophy seems to suggest that ‘to be is to be interactable’, even if that with which we interact is only transient and virtual.


\(^6\) See Floridi (1999), p 43.

\(^7\) See Ess (2007), p 70.

\(^8\) See Floridi (2008b), pp 190-191.
through cyberspace appear to fall outside central international legal doctrines regulating interstate violence, particularly because of the novel forms of harm that they involve. Thus this thesis sought to examine the ways in which states are capable of harming states in and through cyberspace, and how the harm caused by cyber attacks fits in with existing laws regulating interstate violence. The focus was placed on the law on the use of force – the central doctrine through which modern international law seeks to contain the outbreak of interstate conflict and violence.

As demonstrated in chapter 3, while the law has traditionally sought to regulate warfare between the armed forces of states using kinetic weapons causing death and destruction, cyber warfare is premised on different assumptions about the entities, environments, and harm involved in warfare. As such, in exploring the wider context of the law on the use of force, it was demonstrated that the law did not simply arise from the technological context of the time at which the UN Charter was drafted. Instead, it was shown that the law is also premised on different ontological assumptions about the nature of interstate conflict and the forms of violence and coercion that are deemed prohibited in international relations. It was therefore argued that cyber warfare highlights an ontological gap in the existing legal frameworks on warfare, and that the law’s conception of violence is pervaded by an inherently anthropocentric and materialist worldview. Drawing on information ethics, chapter 3 then offered a reconceptualisation of the state as the entity subject to violence and notion of violence in terms of entropy. It was argued that the state entity can be viewed as an information system that continuously receives, processes and communicates information, and increasingly relies on various information flows for its wellbeing and proper functioning as an entity. As a result, even cyber attacks with non-material effects can be seen to harm this entity where they degrade its integrity or undermine its proper functioning. In other words, even non-material cyber attacks constitute a form of informational violence capable of significantly harming the state as an entity.

In chapter 4 it was argued that the law’s ontological constraints are evident in the threshold distinction between the non-use of force and non-intervention principles. Through these distinctions, international law effectively draws the boundaries of what are considered forms of violence and non-violence in interstate relations. As demonstrated by the dominant view within existing legal scholarship in this area, cyber attacks with material effects are considered the easy cases for the use of force analysis as they largely align with the law’s
existing conceptualisation of violence. The more difficult cases arise in relation to cyber attacks without material effects and, as it was shown, there is a tendency in the scholarship to consider these as below the use of force threshold and thus through the non-intervention principle. It was argued that this is due to the law’s ontological constraints – cyber attacks without material effects, such as injury to human beings or damage to physical objects, do not subscribe to the law’s conception of violence. As such, they are effectively equated to forms of non-violence that fall into the periphery of the law’s central discourse regulating interstate violence. Therefore, chapter 4 demonstrated that while the law has the capacity to regulate cyber attacks with material effects, due to its ontologically constrained view of violence, this capacity is limited in relation to cyber attacks without material effects.

In chapters 5 and 6 an informational approach was offered as a means to overcome the law’s ontological constraints that, as was shown in chapter 4, limit the law’s capacity to regulate cyber attacks without material effects in particular. The case study of the 2007 cyber attacks against Estonia in chapter 5 highlighted how the violence inherent in the cyber attacks was evident in the significant increases in entropy they produced. The DDoS attacks in particular undermined the Estonia’s entity’s proper functioning and constituted a form of violence against the Estonian entity. However, as was evident in the majority of the legal analyses of the Estonia incident, the attacks did not cross the use of force threshold and at most breached the non-intervention principle. As such, the violence that Estonia was subject to was not adequately captured by these analyses, and by the general way in which the non-intervention principle is considered in relation to cyber attacks. Instead, an informational approach was used as a way in which to consider the cyber attacks as a form of informational violence causing increased entropy within the Estonian entity, undermining its ability to interact, its autonomy, and its ability to care for and protect the entities within its region of the infosphere.

The Stuxnet case study in chapter 6 in turn demonstrated that, while the law has the capacity to regulate cyber attacks with material effects, an informational approach offers a deeper account of the harm that Stuxnet caused compared to the one-dimensional account of violence evident in existing legal analyses of the incident. Therefore, while Stuxnet is almost universally considered to have constituted a use of force because it caused material damage to centrifuges, the law does not adequately account for Stuxnet’s non-material effects and the forms of informational violence it involved. Here it was shown that an informational
approach offers a means through which both Stuxnet’s material and non-material effects can be considered, as both forms of physical and informational violence that the Iranian entity was subject to and which caused increases in entropy. Stuxnet undermined and degraded the integrity of thousands of entities within Iran’s region of the infosphere, that of the Natanz system which was a key component of Iran’s nuclear program, and consequently also undermined the Iranian entity’s ability to care for and protect the entities within its region of the infosphere. Thus in addition to the material damage it caused to approximately 1000 centrifuges, Stuxnet also caused informational harm to thousands of entities by undermining their integrity and exploiting the interactions between these entities. As such, chapter 6 demonstrated that even where the law has the capacity to regulate cyber attacks with material effects, an informational approach offers a deeper account of violence as it provides the means to consider the material and non-material effects of a cyber attack.

**Information Ethics**

Accordingly, information ethics was used in this thesis to problematise and rethink some of the fundamental tenets of international law in light of the conceptual challenges brought about by ICTs. However, by using information ethics to consider a concrete international problem, this thesis also contributes to the development of information ethics as a field. As highlighted in chapter 2, information ethics has been subject to criticisms – particularly in relation to the ontological equality principle and the notion of entropy as evil. Among these criticisms was the questioning of the reason why all things should have value in themselves, and the practical question of how to assess differences in value between information entities. While Floridi’s responses to these criticisms were outlined in chapter 2, the analysis of the case studies in chapters 5 and 6 also supports the practical viability of an informational approach.

For example, in chapter 5 it was shown that, while the cyber attacks against Estonia affected a range of non-material entities including websites and online services (all of which, pursuant to the ontological equality principle, have a basic right to exist), the overall entropy caused by the attacks could be assessed in terms of the extent to which the attacks on these entities undermined the operation of the Estonian entity as a whole. In this context, the attacks that temporarily undermined the availability of a website, while morally wrong according to the null law of information ethics (entropy should not be caused), would be
considered less wrong as a whole compared to the more widespread DDoS attacks. These attacks undermined the availability of online banking and online access to public services in a state that had heavily integrated the Internet and ICTs into public life. As the analysis of the incident revealed, there was a clear difference between the initial emotional phase of the attacks and the later more organised and sophisticated phase. As such, the Estonia case study offers a practical example of how information ethics can be used to assess the various degrees of entropy caused by cyber attacks.

As to the Stuxnet incident, the overall increases in entropy caused by Stuxnet were evident, for example, in the various ways in which it compromised the integrity of thousands of entities within Iran. Additionally however, it was also possible to consider the differences in value between the key entities involved: Stuxnet and the Natanz enrichment facility. In light of its overall purpose, Stuxnet as a piece of malicious software was an information entity designed to degrade the integrity of another entity. On the other hand, as part of Iran’s nuclear program, the Natanz enrichment facility was designed to enrich uranium. Stuxnet’s goal was therefore to cause entropy in the infosphere (contrary to the null law of information ethics), whereas the Natanz enrichment facility, by enriching uranium for energy production purposes, could be seen as operating in accordance with the laws of information ethics by promoting the flourishing of information entities and the infosphere as a whole. However, as was evident in various UN Security Council resolutions, the international system had effectively deemed the Iranian nuclear program a malicious entity. This was particularly due to the fact that it was operated contrary to international law and because of the overall potential of Iran’s nuclear program in contributing to the production of more significant and widespread increases in global entropy. Viewed in this light, Stuxnet can be seen as designed to prevent entropy and remove potential sources of entropy (aligning with the first and second laws of information ethics), and therefore less morally wrong compared to the operation of the enrichment process. As such, from the perspective of those responsible for Stuxnet’s

---

9 This is pursuant to the moral laws of information ethics, as outlined in chapter 2. While chapter 5 focused on the harm caused by the cyber attacks against Estonia (and not on the morality of the attacks), the moral laws of information ethics can also be used to assess this. Others such as Taddeo and Pagallo have used Floridi’s moral laws to consider the morality of cyber warfare more broadly. See Taddeo (2016), pp 221-222; Pagallo (2015a), pp 416-419.

10 While this thesis was mainly concerned with the harm in cyber attacks (opposed to assessing their morality), the consideration of Stuxnet’s morality was offered as an additional level of analysis. This analysis is informed by Floridi’s moral laws of information ethics and also how these laws have been applied to cyber warfare by Taddeo and Pagallo. See Taddeo (2016), pp 221-222; Pagallo (2015a), pp 416-419. Taddeo for example argues that an entity may lose its right to exist and flourish, and become a legitimate target of cyber warfare, where it
creation, while a malicious entity itself (and, pursuant to existing interpretations of the law, contrary to the prohibition on the use of force provided it caused material damage to centrifuges), Stuxnet can be seen as an entity designed to undermine the operation of another more malicious entity.

Accordingly, as both the Estonia and Stuxnet case studies illustrate, information ethics can be applied in concrete situations to consider the entropy caused to a range of information entities and also assess the differences in the degrees of entropy produced. Especially given the nature of these incidents and because the issues they raise would not have been possible prior to the development of modern ICTs, the case studies illustrate that the expansion of ethical concern beyond human beings and material objects to also purely informational entities and processes has practical utility too, for instance, when considering the harm caused by cyber attacks.

**International Law**

In addition to this contribution to information ethics as a field, the informational approach developed in this thesis can be used to think about law, technology and violence more generally. As demonstrated in this thesis, information ethics provides a conceptual basis on which to rethink the law’s anthropocentrism and materialism in informational terms. Beyond cyber attacks and the law on the use of force, this is useful given the range of issues that new technologies are raising for the law, for instance, in relation to various non-human entities that are capable of operating with increasing levels of autonomy. Recognising a broader range of entities as having moral value also raises questions about the role and purpose of the state, and whether it has a responsibility to care for and protect, not only human entities, but all entities within its region of the infosphere. Further, where states engage in activities that are harmful to these entities, the violence inherent in the degradation or destruction of information entities can be seen in a way that is not limited by the law’s existing worldview.

Prior to considering some of the wider implications of an informational approach for international law, and discussing other sites of the law’s intersection with technology where

---

endangers or disrupts the wellbeing of the infosphere. In this context, because of the potential of Iran’s nuclear weapons program to endanger the wellbeing of the infosphere, it would be morally justified to remove this entity and prevent it from causing evil. Further, Stuxnet could be seen as more moral than a traditional military strike on the Natanz facility as this would likely have involved human casualties and more significant physical destruction. Therefore, in this context, Stuxnet could be seen as a form of ‘just informational violence,’ despite being generally considered to have breached international law on the use of force.
future research may be undertaken, it is worth briefly considering some of the practical ways in which the law on the use of force can be reformed.

Law and Informational Violence

Considering informational violence and the law more broadly, there are fundamental differences in terms of how the law conceives this violence and its legality. Often this depends on the actors responsible. For example, where non-state actors engage in activities involving forms of informational violence, such as obtaining unauthorised access to computers and information or launching DDoS attacks against websites, these acts are considered through criminal law and hence through the domestic laws of the state. Where state actors or non-state actors under the control of states do so, depending on the exact targets and the general motivations of those responsible, the violence can be conceptualised very differently. For instance, where the targets are corporate entities and the information that is undermined is commercially sensitive, this informational violence can be classed as economic espionage. In contrast, where the targets are government databases and politically sensitive information is compromised, then it tends to be seen merely as a form of political espionage which international law traditionally has little to say about. However, these distinctions and classifications are not always clear cut, especially given issues around anonymity and the potential involvement of a multitude of actors. Where cyber attacks involve more significant degrees of informational violence however (or even physical violence), and provided they can be attributed to state actors, then the law on the use of force and non-intervention become potentially applicable. Accordingly, the entities responsible for activities involving informational violence, the nature of the entities subject to harm, and the degree of harm in question, greatly impact on how the law conceptualises this violence and whether it is deemed illegal or implicitly permitted or condoned. Thus if a non-state actor

12 For example, in 2015 the personal details of 21.5 million current and former US federal employees (including fingerprints of over 5 million people) were compromised by a ‘Chinese espionage operation’, see ‘US government hack stole fingerprints of 5.6 million federal employees’, The Guardian, 24 September 2015.
13 For example, in 2014 the Sony Corporation’s computer systems were compromised and large amounts of data were stolen or deleted. A non-state actor group claimed responsibility for the incident, and it is believed they acted with the support of North Korean state agencies. In response, the US government issued sanctions against North Korean officials. See Barnes and Cieply, ‘Sony Cyberattack, First a Nuisance, Swiftly Grew Into a Firestorm’, The New York Times, 30 December 2014; Zetter, ‘Sony Got Hacked Hard: What We Know and Don’t Know So Far’, Wired, 3 December 2014; Sanger and Schmidt, ‘More Sanctions on North Korea After Sony Case’, The New York Times, 2 January 2015.
without state support obtains unauthorised access to a government’s databases and the incident is considered through criminal law, it is effectively deemed a form of illegal and illegitimate informational violence. In contrast, when a government collects information about individuals or corporations in another state, or accesses information stored in another government’s databases without authorisation, without law specifically deeming this illegal, the informational violence is effectively deemed legitimate.

In effect, within cyberspace, the law currently enables states to relatively freely engage in activities involving violence, whereas the law is used to restrict non-state actors from doing so. This can be seen as an affirmation of the state’s monopoly of violence over forms of informational violence. By criminalising engagement in informational violence by non-state actors through their domestic laws, states can monopolise informational violence through the law. Internationally however, instead of bringing it within the law regulating interstate violence and into a legal monopoly of violence, informational violence is left outside the law’s conception of violence. Accordingly, as a form of violence outside how the law sees violence on the international level, states are effectively enabled to engage freely in activities involving informational violence. Therefore, while the criminalisation of informational violence by non-state actors is express, implicit in this is a more subtle establishment of a monopoly of informational violence outside the law.\textsuperscript{14} States are in effect exploiting not only vulnerabilities in ICTs, but also exploiting international law’s incapacity to regulate cyber attacks involving novel forms of harm.

By viewing informational violence through the use of force principle, the informational nature and harm of these attacks towards states as information systems can be taken more seriously. Michael Schmitt for example, in relation to the future development of the law on the use of force, has argued that:

as cyber activities become ever more central to the functioning of modern societies, the law is likely to adapt by affording them greater protection. It will impose obligations on states to act as responsible inhabitants of cyberspace, lower the point at which cyber operations violate the prohibition on the use of force, allow states to

\textsuperscript{14} David Fidler, for example, has suggested that Stuxnet’s development and use by the US and Israel may see the development of international law into the direction of ‘cyber-specific rules that increase the political and legal space in which states can use cybertechnologies against one another’ – rules that push established boundaries of the use of force threshold permitting states ‘to explore and exploit cybertechnologies as instruments of foreign policy and national security.’ Fidler (2011), p 58.
respond forcefully to some non-destructive cyber operations, and enhance the protection of cyber infrastructure, data, and activities during armed conflicts.\textsuperscript{15}

In essence, as information becomes more and more central, the law too will need to recognise informational violence as capable of harming state entities. Not only does informational violence involve damage to data or the disruption of information systems, but it also constitutes a form of violence against the state as an information entity. Specific ways in which the law can be reformed include, for example, incorporating into the Tallinn Manual’s criteria on the assessment of when a cyber attack constitutes a use of force, a need to consider the degrees of increases in entropy caused by a cyber attack when assessing its ‘severity’;\textsuperscript{16} and the amount of entities harmed, and how important they are to the functioning of a state, when considering a cyber attack’s ‘invasiveness’ and ‘measurability’.\textsuperscript{17} Additionally, the moral laws of information ethics also offer general principles to guide the behaviour of states as ‘responsible inhabitants of cyberspace’, or as responsible and caring agents in the infosphere.\textsuperscript{18}

Implicit in this is also a normative assumption about the ability of law to regulate violence, and that informational violence ought to be regulated, once it can be recognised. To some extent this is a normative argument about the future development of law. However, as the case studies demonstrated, the use of cyber attacks involving only informational or both informational and physical forms of violence that are capable of disrupting the functioning of ICT dependent societies or their industrial programs is a current and real concern for the law. It is unlikely that these developments would have been within the contemplation of the drafters of the UN Charter, despite early predictions about the future social and ethical impact of computers.\textsuperscript{19} As a result, activities that are not traditionally conceived of as harmful or as forms of violence, including various activities occurring in and through cyberspace that undermine the informational integrity or proper functioning of information societies, can be reconceptualised as informational violence and brought within the law’s conceptual containment of violence.

\textsuperscript{15} Schmitt (2014), p 299.
\textsuperscript{16} This is similar to what Pagallo has suggested, namely that the informational or virtual severity of an attack should be taken into account. See Pagallo (2015a), pp 414-415.
\textsuperscript{17} For all the Tallinn Manual criteria, see part two of chapter 4.
\textsuperscript{18} Pagallo (2015a), pp 416-419.
\textsuperscript{19} Such predictions were made, for example, by Norbert Wiener in the 1940s. See Bynum (2008a), pp 25-26.
An Informational Approach

In chapter 3, an alternative image of the state was offered. Viewed in informational terms, the essence of the state entity was described as coming from its primary purpose: to care for and protect all entities within its region of the infosphere. Therefore, as a responsible and caring inhabitant of the infosphere pursuant to the laws of information ethics, the state has a responsibility to do so. In the wider context of international law, the notion of ‘responsibility to protect’ emerged at the beginning of the twenty-first century in human rights law as the idea that state entities have a responsibility to protect human beings within their territories.\(^{20}\)

On the other hand, in international environmental law, the notion of sustainable development emerged in the late twentieth century as the idea that the natural resources on which present and future generations depend should be also protected.\(^{21}\) The idea of the responsibility to care for and protect all entities within a state’s region of the infosphere is a conscious amalgamation of the basic ideas behind these concepts and their extension to the infosphere. On a premise broader and more inclusive than human or state equality, drawing on the notion of ontological equality, this extends the idea that not only human beings or the natural environment should have rights and be protected, but that everything by virtue of its existence has a (basic) right to exist and flourish according to its nature. This means that, as a starting point, state entities should have a responsibility to care for and protect all entities within their region of the infosphere. It does not mean that the rights of databases or natural resources will always trump those of human beings, but simply that when viewed informationally, the rights of all entities can be taken into consideration. As such, the notion of a responsibility to care for and protect seeks to capture a concern for the wellbeing of the recipient of actions, and for all the entities involved in their interactions, as the premise of what is considered good within the global infosphere.

By expanding the scope of the notion of violence to a broader ontological spectrum, the potential of states to inflict harm through their various activities in and through cyberspace against a range of entities can be appreciated in a new light. Like nuclear weapons technologies that demonstrated the novel technological capacity of states to annihilate entire cities, while the full extent of states’ offensive cyber attack capabilities are unknown, incidents such as Stuxnet offer glimpses into these capabilities and the future of interstate

\(^{20}\) Where the state fails to do so, then the responsibility shifts to the international community. Orford (2011), pp 1-2.
violence. While Stuxnet, for example, was designed to limit collateral damage as it only targeted very specific computer configurations and caused damage subtly, it could have been designed differently. It could have been designed to cause less discriminate harm, more immediate physical damage, or more widespread and significant informational harm. This could have involved, for instance, deletion of the data in the computers it spread to. While the law would not traditionally regard the intentional destruction of data as a form of violence, from an informational perspective it could be seen as a large scale informational cleansing of sorts. As such, by expanding the ontological scope of the notion of violence, the harmful potential of states’ offensive cyber attack capabilities can be appreciated within the context of the increasing ICT dependency of information societies.

To a degree this ‘infocentric’ shift in focus can be seen as a dislodgment of the human which is at the very foundation of law. Both human rights law and humanitarian law, for example, are premised on fundamental assumptions about what entities constitute human beings that, through the provision of rights, should be protected from violence. The aim here is not to trivialise the notion of violence and equate the deletion of data to the killing of human beings in terms of moral reprehensibility. Instead, as a means of rethinking the law’s anthropocentrism and materialism that were shown to limit the law’s capacity to regulate interstate violence, an informational approach offers a change of perspective. Indeed, it is worth noting that in human rights law, and law more generally, while usually seen as formally equal under the law, even human beings are distinguished in terms of their substantive differences. As such, regardless of any formal depiction of humans as information entities (as information organisms or inforgs in Floridi’s words) that enjoy a basic right to exist shared by all other information entities, even when humans are seen informationally they can still be seen as uniquely complex information structures. It thus remains possible to make distinctions between these complex information structures, for example, on the basis of their information communication and processing abilities. Even the law does this in relation to the entities that are given a right to political participation, for example, as distinctions are based on a human being’s age and mental capacity. Therefore, this ‘infocentrism’ does not necessarily reduce human beings to mere information entities, instead it simply offers a perspective from which to consider all entities (including human beings) in similar terms. As such, it not only broadens the scope of the entities capable of being considered subject to harm, but also the scope of the entities capable of performing actions and having legal agency. This is especially useful given the ways in which artificial and increasingly
autonomous entities – such as driverless cars, killer robots and other non-human entities – are raising novel legal issues in many areas of the law. As such, while it may problematise the law’s anthropocentrism, in doing so it allows for consideration of the various non-human entities that have the information processing and communication abilities to increasingly perform actions previously reserved purely to human beings as legal agents.\textsuperscript{22}

Finally, it is worth returning to the ideas of Gorniak-Kocikowska and Kanuck that were outlined at the beginning of this chapter. Specifically, it was predicted that the future ethic will be global in the spatial sense, and it was proposed that international law’s next conceptual paradigm needs to shift away from territory towards information and interactions. Against international law’s universalism – historically, a particular European universalism\textsuperscript{23} – information ethics offers a uniquely universal foundation for the law that is based on information. From an informational perspective, the informational substance that all entities share is universal. With this as the law’s conceptual foundation and its universal premise, a readjustment of the law’s focus away from the human individual and the territorial state is required. This enables a shift in its conceptual foundation towards information and interactions. In international law, by considering states as information entities that increasingly interact with other entities within the global infosphere, law can be designed with a concern for the ‘quality and healthiness’ of the interactions between these entities and their contribution to the enrichment of the infosphere.\textsuperscript{24} As such, the focus shifts away from the traditional account in which territory is seen as the essence of the state’s existence and the law’s conceptual basis,\textsuperscript{25} towards one based on the interactions of information entities. Beyond cyber attacks and the use of force, this means various other activities can be considered within the same conceptual framework in terms of their impact on the infosphere. As such, from trade restrictions to online censorship and environmental pollution, the potential entropy and the degree to which these activities enrich the wellbeing of the global infosphere can be considered. Also beyond state activities, from individuals to corporations and international organisations, a wider range of entities that increasingly interact within the international system can be brought within the same conceptual umbrella. Therefore, by offering a conceptual framework based on information that is truly global in the spatial sense,

\textsuperscript{22} Floridi and Sanders, for instance, examine the concept of agency in relation to artificial agents, see Floridi and Sanders (2004b). As to legal agents, Mireille Hildebrandt et al consider whether, for example, software agents and robots should be given some form of limited legal personhood. Hildebrandt et al (2010).

\textsuperscript{23} See, for example, Jouannet (2007), pp 380-382.

\textsuperscript{24} The Onlife Initiative (2015), p 46.

\textsuperscript{25} See Cassese (2005), p 81. See also chapter 3.
information ethics has the ability to offer a new paradigm for law regulating interactions in the information age.

In conclusion, this thesis drew on information ethics to examine the conceptual challenge brought about by cyber attacks to how the notion of violence is understood in international law on the use of force. It was argued that the reasons for this challenge are ontological, as the law embodies an anthropocentric and materialist conception of violence and the state as an entity. The ability of states to use cyber attacks against other states, within the wider context of the transformations and challenges brought about by ICTs, invited an informational reconceptualisation of the notion of violence and the state as the entity subject to violence. The state was described as a dynamic entity that relies on various flows of information for its proper functioning, and cyber attacks causing increases in entropy as forms of violence against this entity. Therefore, it was argued that an informational reconfiguration of the law’s ontological constraints provides a way in which to recognise how informational violence is also capable of harming the state.
Bibliography

Secondary Sources


Ian Brownlie (1963) International Law and the Use of Force by States, Oxford University Press.


Anthony D'Amato (1990) ‘The Invasion of Panama was a Lawful Response to Tyranny’ 84(2) *American Journal of International Law* 516.


Christopher Barth Kuner (2013) Transborder Data Glows and Data Privacy Law, Oxford University Press.


Primary Sources

Cases, Treaties and Legislation


Harmful Digital Communications Act 2015 (New Zealand).


International Convention with Respect to the Laws and Customs of War on Land, opened for signature 29 July 1899, [1901] ATS 131 (entered into force 4 September 1900).


_SS ‘Lotus’ (France v Turkey) (Judgment) [1927] PCIJ (series A) No 10._


_United Nations Documents_

_Creation of a Global Culture of Cybersecurity_ (adopted by the UN General Assembly on 31 January 2003, UN Doc A/RES/57/239).


_Creation of a Global Culture of Cybersecurity and the Protection of Critical Information Infrastructures_ (adopted by the UN General Assembly on 21 December 2009, UN Doc A/RES/64/211).
Declaration on Principles of International Law Concerning Friendly Relations and Co-operation among States in Accordance with the Charter of the United Nations (adopted by the UN General Assembly on 24 October 1970, UN Doc A/RES/2625(XXV)).

Declaration on the Enhancement of the Effectiveness of the Principle of Refraining from the Threat or Use of Force in International Relations (adopted by the UN General Assembly on 18 November 1987, UN Doc A/RES/42/22).

Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of their Independence and Sovereignty (adopted by the UN General Assembly on 21 December 1965, UN Doc A/RES/20/2131(XX)).

Definition of Aggression (adopted by the UN General Assembly on 14 December 1974, UN Doc A/RES/29/3314).


Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, Report of the Group of Governmental Experts on Developments in the Field of Information and


The Right to Privacy in the Digital Age (adopted by the UN General Assembly on 18 December 2013, UN Doc A/RES/68/167).


Newspapers and Magazines


Other


