The 2007 Cyber Attacks Against Estonia and International Law on the Use of Force: An Informational Approach

Samuli Haataja*

* BIntRel, LLB(Hons), PhD. Adjunct, Law Futures Centre, Griffith Law School, Griffith University, Gold Coast, Australia. I would like to thank Kieran Tranter and Afshin Akhtarkhavari for their comments on earlier versions.

s.haataja@griffith.edu.au
orcid.org/0000-0003-3528-6013

Word count: 15,107

The 2007 Cyber Attacks Against Estonia and International Law on the Use of Force: An Informational Approach

This article considers the 2007 cyber attacks against Estonia and international law on the use of force. It argues that the prohibition on the use of force in Article 2(4) of the United Nations Charter embodies an ontologically constrained conceptualisation of violence that requires some form of material damage to property or injury or death of human beings. As a result, the law is incapable of adequately recognising the harm caused by cyber attacks with non-material effects like those against Estonia. In an effort to overcome these constraints, this article draws on Luciano Floridi's information ethics. This theory extends its ethical concern beyond the material world to include all entities, whether natural or artificial, physical or virtual. It is argued that by viewing the Estonian entity as an information system, the 2007 cyber attacks can be seen to have constituted a form of informational violence against this entity.

Keywords: cyber attacks, use of force, Estonia, information ethics

Introduction

In September 2007, in an address to the United Nations (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]

In April and May of 2007 Estonia had become subject to a new form of 'cyber violence.' It became the first nation-state subject to large-scale distributed denial of service (DDoS)

[1] Toomas Hendrik Ilves, 'Address by the President of Estonia' (62nd Session of the United Nations General Assembly, New York, 25 September 2007) <http://www.un.org/webcast/ga/62/2007/pdfs/estonia-eng.pdf> accessed 15 November 2016.

attacks in what was widely described in the media as a 'cyber war'[2] and what Estonia's President later depicted as 'Web War One.'[3] The cyber attacks were triggered by the government's decision to relocate a politically contentious war memorial statue from the centre of Tallinn to a nearby military cemetery. This caused anger among Estonia's ethnic Russians and their supporters in Russia, leading to protests and riots in the streets of Tallinn, and ultimately to multiple waves of cyber attacks lasting over three weeks in total.[4] Estonia was particularly vulnerable to the threat of cyber attacks given the degree to which it had integrated Internet based solutions into most aspects of public life already in 2007. Everything from filing social security and tax claims occurred entirely digitally, and voting was also possible in local elections at the time.[5] The cyber attacks targeted various Estonian websites including those of the President, Prime Minister, Parliament, most government departments,[6] political parties, media organisations, banks and Internet Service Providers (ISPs).[7] They also targeted Estonia's Internet infrastructure and information systems, such as

[2] The Washington Post described it as 'cyber-warfare' (see 'Pushback for Mr. Putin' *The Washington Post* (Washington, 19 May 2007) <http://www.washingtonpost.com/wp-dyn/content/article/2007/05/18/AR2007051801722.html> accessed 15 November 2016) as did The Guardian (see Ian Traynor, 'Russia accused of unleashing cyberwar to disable Estonia' *The Guardian* (London, 17 May 2007) <https://www.theguardian.com/world/2007/may/17/topstories3.russia> accessed 15 November 2016). The New York Times depicted it as 'the first war in cyberspace' (Mark Landler and John Markoff, 'Digital Fears Emerge After Data Siege in Estonia' *The New York Times* (New York, 29 May 2007) <http://www.nytimes.com/2007/05/29/technology/29estonia.html?_r=0> accessed 15 November 2016) whereas Slate used the term 'cyberwar I' (see Cyrus Farivar, 'Cyberwar I' *Slate* 22 May 2007) <http://www.slate.com/articles/technology/technology/2007/05/cyberwar_i.html> accessed 15 November 2016).

[3] Toomas Hendrik Ilves, 'Address by the President of Estonia' (67th Session of the United Nations General Assembly, New York, 26 September 2012) <https://vp2006-2016.president.ee/en/official-duties/speeches/7991-address-by-h-e-toomas-hendrik-ilves-president-of-estonia-to-the-67th-session-of-the-united-nations-general-assembly-un-headquarters-new-york-september-2012/> accessed 31 January 2017.

[4] Traynor (n 2).

[5] Eneken Tikk, Kadri Kaska and Liis Vihul, *International Cyber Incidents: Legal Considerations* (NATO Cooperative Cyber Defence Centre of Excellence 2010) 16-18.

[6] For a list, see Jose Nazario, 'Estonian DDoS Attacks – A summary to date' (*Arbor Networks*, 17 May 2007) <https://www.arbornetworks.com/blog/asert/estonian-ddos-attacks-a-summary-to-date> accessed 15 November 2016.

[7] Landler and Markoff (n 2); Christopher Rhoads, 'Estonia Gauges Best Response To Cyber Attack' *The Wall Street Journal* (New York, 18 May 2007) A6; Traynor (n 2); Ian Traynor, 'Web attackers used a million computers, says Estonia' *The Guardian* (London, 18 May 2007) <https://www.theguardian.com/technology/2007/may/18/news.russia>; Peter Finn, 'Cyber Assaults on Estonia Typify a New Battle Tactic' *The Washington Post* (Washington, 19 May 2007) <http://www.washingtonpost.com/wp-dyn/content/article/2007/05/18/AR2007051802122.html> accessed 15 November 2016).

the national Domain Name Service (DNS) and the DNSs operated by various ISPs.[8] The primary effect of the attacks was disruptive. They disrupted access to various websites and the services they provided, affected the operation of government communication channels,[9] and caused slight interruptions to mobile networks[10] and to the emergency services line.[11] The disruptions are reported to have seriously impaired the daily operation of various organisations including banks, government departments, and small businesses.[12] The online communication channels between the government and Estonians were also temporarily impaired and, given the degree to which important public services were only accessible online, the lack of access to these services had a 'discernible effect' for many people.[13] Some estimates quantify the economic impact of the attacks at between twenty-seven to forty million United States (US) dollars.[14]

As some of the attacks were traced to Russian Internet Protocol (IP) addresses, Estonia initially blamed Russia for the attacks. Its Minister of Foreign Affairs, for example, maintained that Estonia was under attack from Russia that was 'virtual, psychological and real – all at the same time.'[15] The Prime Minister also claimed that the sovereign state of Estonia was 'under a heavy attack.'[16] Despite initial allegations by Estonian officials that Russia was responsible for the attacks, Russia has denied its involvement.[17] Ultimately the incident was dealt with as a criminal matter, though only one twenty year old Estonian

[8] Tikk, Kaska and Vihul (n 5) 21.
[9] ibid 22.
[10] ibid 22.
[11] 'Marching off to cyberwar' *The Economist* (London, 4 December 2008) <http://www.economist.com/node/12673385> accessed 15 November 2016.
[12] Tikk, Kaska and Vihul (n 5) 24.
[13] ibid 25.
[14] See Sheng Li, 'When Does Internet Denial Trigger the Right of Armed Self-Defense?' (2013) 38 *Yale Journal of International Law* 179, 200.
[15] 'Declaration of the Minister of Foreign Affairs of the Republic of Estonia' (*Republic of Estonia Government*, 1 May 2007) <https://valitsus.ee/en/news/declaration-minister-foreign-affairs-republic-estonia> accessed 15 December 2016.
[16] 'Prime Minister Andrus Ansip's speech in Riigikogu' (*Republic of Estonia Government*, 2 May 2007) <https://valitsus.ee/en/news/prime-minister-andrus-ansips-speech-riigikogu> accessed 15 December 2016.
[17] Charles Clover, 'Kremlin-backed group behind Estonia cyber blitz' *Financial Times* (Tokyo, 11 March 2009) <http://www.ft.com/intl/cms/s/0/57536d5a-0ddc-11de-8ea3-0000779fd2ac.html> accessed 15 November 2016.

student was fined for launching an attack against one of the targeted websites.[18] Some experts believe, however, that the only plausible explanation is that the Russian government gave some degree of approval for the actions of those conducting the cyber attacks.[19] Others maintain that it is impossible to prove who was or was not responsible for the attacks based on the technical information available.[20]

In addition to the Estonia incident, in recent years there have been a host of malevolent activities in and through cyberspace involving state actors.[21] These range from the release of Stuxnet – a piece malicious software created by the US and Israel believed to have been responsible for physically destroying nuclear centrifuges in Iran around 2010,[22] to non-destructive activities compromising the integrity of information stored in computers. Recently, for example, an alleged Chinese espionage operation compromised the personal data of approximately 21.5 million US federal employees in 2015,[23] and Russian intelligence agencies allegedly obtained unauthorised access to information in the US Democratic Party's computers during the 2016 presidential election.[24]

Incidents such as these have exposed limitations in existing laws regulating interstate activities and contributed to a sense of anxiety about the threat of cyber attacks. While

---

[18] 'Estonia fines man for 'cyber war'' *BBC News* (London, 25 January 2008) <http://news.bbc.co.uk/2/hi/technology/7208511.stm> accessed 15 November 2016. See also Clark Boyd, 'Cyber-war a growing threat warn experts' *BBC News* (London, 17 June 2010) <http://www.bbc.co.uk/news/10339543> accessed 15 November 2016.

[19] Rain Ottis, 'Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective' in Dan Remenyi (ed), *Proceedings of the 7th European Conference on Information Warfare and Security* (Academic Publishing Limited 2008).

[20] Gadi Evron, 'Authoritatively, Who Was Behind The Estonian Attacks' (*Dark Reading*, 17 March 2009) <http://www.darkreading.com/risk/authoritatively-who-was-behind-the-estonian-attacks/d/d-id/1130584> accessed 15 November 2016.

[21] For a list of significant cyber attacks since 2006, see 'Significant Cyber Incidents' (*Center for Strategic and International Studies*) <https://www.csis.org/programs/strategic-technologies-program/cybersecurity/significant-cyber-incidents> accessed 15 November 2016.

[22] See David Albright, Paul Brannan and Christina Walrond, *Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?* (Institute for Science and International Security, 22 December 2010).

[23] 'US government hack stole fingerprints of 5.6 million federal employees' *The Guardian* (London, 24 September 2015) <https://www.theguardian.com/technology/2015/sep/23/us-government-hack-stole-fingerprints> accessed 15 November 2016.

[24] Eric Lichtblau, 'Computer Systems Used by Clinton Campaign Are Said to Be Hacked, Apparently by Russians' *The New York Times* (New York, 29 July 2016) <http://www.nytimes.com/2016/07/30/us/politics/clinton-campaign-hacked-russians.html?_r=2> accessed 15 November 2016.

international law prohibits states from using 'force' in their international relations,[25] this is generally understood to require some degree of damage to physical objects or injury to human beings.[26] As such, a prominent issue raised by states engaging in malevolent cyber activities is whether these new forms of 'cyber violence' fall within existing laws regulating interstate violence, particularly where their effects do not amount to what is traditionally understood as 'violence.'[27] While Stuxnet is the first publicly known example of a cyber attack causing physical damage in the real world, non-destructive or mainly disruptive cyber attacks are more problematic. This is particularly due to the fact that, like the attacks against Estonia and the incidents mentioned above, these cyber attacks did not involve direct injury to human beings or damage to material objects.

This article considers the 2007 cyber attacks against Estonia and international law on the use of force. It is specifically concerned with the harm or damage caused by cyber attacks like those against Estonia, in the context of the threshold question of when a cyber attack amounts to a use of force under Article 2(4) of the UN Charter. It is argued that international law in this context embodies an ontologically constrained conceptualisation of violence that requires some form of material damage to property or injury or death of human beings. As a result, the law is incapable of adequately recognising the harm caused by cyber attacks with non-material effects, such as those against Estonia. Drawing on Luciano Floridi's information ethics – a theory that extends its concern beyond human beings and the natural environment to all information entities and environments – an informational approach is offered as an innovative way in which to think about the harm caused by cyber attacks. It is argued that this provides a means to consider non-material cyber attacks as a form of 'informational violence'

[25] UN Charter, Article 2(4).
[26] See, for example, Yoram Dinstein *War, Aggression and Self-Defence* (5th edn, Cambridge University Press 2011) 88.
[27] See, for example, Thomas Rid, *Cyber War Will Not Take Place* (Oxford University Press 2013) 12-13.

capable of harming virtual entities and processes, even where no human beings or material objects are harmed.

This article consists of two sections. The first section examines the law on the use of force under Article 2(4) of the UN Charter, and how the law is considered to apply to cyber attacks generally and in relation to the Estonia incident in particular. The second section provides an overview of Floridi's information ethics and develops an informational approach to the Estonia incident. It will be shown that by viewing the Estonian state entity as an information entity with a responsibility to care for and protect its region of the 'infosphere,' the cyber attacks that Estonia was subject to can be seen as harming it by causing 'entropy' and disrupting its normal operation as an entity.

I Cyber attacks, the use of force and non-intervention

This section first provides an overview of how the notion of 'force' within Article 2(4) of the UN Charter is understood, and how the law is considered to extend to cyber attacks. It then considers the non-intervention principle and cyber attacks below the use of force threshold, and it examines how the cyber attacks against Estonia are characterised in existing legal scholarship. It is argued that the law reflects an ontologically constrained view of violence because it is incapable of seeing the effects of non-material cyber attacks as a form of harm within the Article 2(4) conception of 'force.' Instead, violence in this context requires some form of injury to human beings or damage to physical property. Consequently, disruptions to the functioning of non-material entities – virtual entities and processes, such as websites and networks – is not a form of harm the law is capable of recognising.

Cyber attacks and the use of force

Traditionally the state is conceptualised as a fixed territorial entity with sovereignty.[28] It is often described in anthropomorphic terms,[29] with its territorial 'body' providing the container of modern society that separates its internal or domestic affairs from its external or foreign affairs.[30] This imagery of the state as a person or actor is also evident in international law.[31] 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.[32] Without these features, an entity is generally not considered a state.[33] Territory is a particularly important element of statehood as 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.[34]

---

[28] For example, Eve Darian-Smith notes how more generally in traditional scholarship on the state, '[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.' Eve Darian-Smith, *Laws and Societies in Global Contexts: Contemporary Approaches* (Cambridge University Press 2013) 179.

[29] This image pervades literature on the state as the state is depicted as an individual 'actor' or 'person' with an identity and interests, and holding 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.' Erik Ringmar, 'On the Ontological Status of the State' (1996) 2 *European Journal of International Relations* 439, 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. Alexander Wendt, 'The State as Person in International Theory' (2004) 30 *Review of International Studies* 289, 289.

[30] 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.' Anthony Giddens, *The Nation-State and Violence* (Polity Press 1985) 13. See also Peter J Taylor, 'The State as Container: Territoriality in the Modern World-System' (1994) 18 *Progress in Human Geography* 151. 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.' John Agnew, *Geopolitics: Re-Visioning World Politics* (Routledge 1998) 51.

[31] According to Antonio Cassese for example, states are 'the *dramatis personae* (the characters of the play) on the international scene'. He also describes how insurgents 'are born from a wound in the body of a particular State.' Antonio Cassese, *International Law* (Oxford University Press 2005) 71.

[32] See Montevideo Convention on Rights and Duties of States, 26 December 1934, 136 LNTS 19, Article 1.

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

[34] See Cassese (n 31) 81. He writes that:

States, in their international relations, are prohibited from using violent means to solve their disputes. This is in contrast to earlier times in which the resort to forceful means was considered a sovereign prerogative, as existing rules limit the capacity of states to use force.[35] Article 2(4) provides that all UN member states:

> 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.[36]

For the purposes of the present article, the primary concern is with the notion of 'force' within Article 2(4).[37] This ambiguous notion is not defined within the UN Charter and there has been debate about its meaning.[38] For example, when Article 2(4) was drafted the Brazilian delegation suggested that in addition to military action it should also include economic coercion, however, this view was rejected at the time.[39] Also, because elsewhere in the UN Charter the words 'armed force' are used instead of simply 'force', there has been debate about how it should be interpreted within the context of the UN Charter.[40]

> 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.

[35] Yoram Dinstein, *War, Aggression and Self-Defence* (3rd edn, Cambridge University Press 2001) 71.

[36] UN Charter, Article 2(4).

[37] There are various other elements within this provision. Article 2(4) also prohibits 'threats' of force; it is only considered to apply to international (opposed to internal) conflicts; it also applies to 'indirect' uses of force; and the phrase 'against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations' is not deemed to limit the scope of the provision. See, generally, Albrecht Randelzhofer, 'Article 2(4)' in Bruno Simma and others (eds), *The Charter of the United Nations: a Commentary* (Volume 1, Oxford University Press 2002). See also Ian Brownlie, *International Law and the Use of Force by States* (Oxford University Press 1963) 267; Leland Matthew Goodrich, Anne Patricia Simons and Edvard Isak Hambro, *Charter of the United Nations: Commentary and Documents* (3rd and revised edn, Columbia University Press 1969) 50; Bert V A Röling, 'The Ban on the Use of Force and the U.N. Charter' in Antonio Cassese (ed), *The Current Legal Regulation of the Use of Force* (Martinus Nijhoff Publishers 1986) 4; Dinstein (n 35) 80-82; Malcolm N Shaw, *International Law* (7th edn, Cambridge University Press 2014) 817.

[38] Randelzhofer (n 37) 117; Michael N Schmitt, 'Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework' (1999) 37 *Columbia Journal of Transnational Law* 885, 904.

[39] Randelzhofer (n 37) 118; Schmitt (n 38) 905.

[40] Albrecht Randelzhofer for instance argues that because the term 'armed force' is used throughout the UN Charter, Article 2(4) must refer to that too. Randelzhofer (n 37) 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 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 Heather

Despite these debates, the prevailing view is that force only refers to *armed* force. This has been interpreted to extend to non-kinetic weapons such as chemical and biological agents,[41] and destructively used non-military force (such as releasing large quantities of water or spreading fires).[42] Similarly, the International Court of Justice (ICJ) has highlighted that it does not matter what type of weapons are employed for the provision to apply.[43]

On the question of when a cyber attack constitutes a use of force, with 'hard' international law lacking in this area, the *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Tallinn Manual) provides an important soft-law instrument to guide this determination.[44] Rule 11 of the Tallinn Manual states that:

> A cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force.[45]

As such, pursuant to the Tallinn Manual a cyber attack (operation) will constitute a use of force when it is comparable in 'scale and effects' to a traditional use of armed force. In the commentary to the rules, the authors note that generally '[a]cts that injure or kill persons or damage or destroy objects are unambiguously uses of force'[46] and where cyber attacks have similar consequences, they are 'highly likely' to constitute uses of force.[47] The authors also

---

Harrison Dinniss, *Cyber Warfare and the Laws of War* (Cambridge University Press 2012) 41. Others adopt a different line of reasoning and distinguish the instances in which the UN Charter refers to armed force specifically, and argue that force within Article 2(4) is not limited to armed force. For instance according to Hans Kelsen, the term 'is meant to include not only armed force, but any illegal action of one state which violates the legally protected interests of another'. Hans Kelsen, *Collective Security Under International Law* (The Lawbook Exchange, Ltd. 2001) 55.

[41] Brownlie (n 37) 362.

[42] ibid 362-363, 376. See also Randelzhofer (n 37) 118-119.

[43] *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion, 8 July 1996, ICJ Reports 1996, 226, para 39.

[44] Michael N Schmitt (ed), *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press 2013).

[45] ibid 45.

[46] ibid 48.

[47] ibid 48.

provide a number of factors that can be considered in making the assessment.[48] Here too they stress that the severity of an attack is the 'most significant' criterion to be considered.[49]

Like in the Tallinn Manual, the effects of a cyber attack are also of particular relevance within the legal scholarship on the issue of when a cyber attack crosses the use of force threshold. While three general approaches are evident in this literature that focus on the cyber attack's targets, the instruments used, and their effects respectively, the 'effects approach' has attracted most support.[50] 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, however, more recent views only consider those attacks with tangible effects as qualifying.[51] 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. Jason 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.[52] Michael 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.'[53] For Heather Harrison Dinniss 'it appears to be clear' that a cyber attack will

[48] These are 1) severity, 2) immediacy, 3) directness, 4) invasiveness, 5) measurability, 6) military character, 7) state involvement, and 8) presumptive legitimacy. See ibid 48-51. These criteria are based on the six criteria that Michael Schmitt first suggested in the late 1990s. Schmitt (n 38) 914-915.

[49] Schmitt (ed) (n 44) 48. They also noted that the severity of an attack is influenced by its scope, duration and intensity.

[50] 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. 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. See Marco Roscini, *Cyber Operations and the Use of Force in International Law* (Oxford University Press 2014) 47; Duncan B Hollis, 'Why States Need an International Law for Information Operations' (2007) 11 *Lewis & Clark Law Review* 1023, 1041; Oona A Hathaway and others, 'The Law of Cyber-Attack' (2012) 100 *California Law Review* 817, 846-847; David E Graham, 'Cyber Threats and the Law of War' (2010) 4 *Journal of National Security Law and Policy* 87, 91.

[51] Walter Gary Sharp, *CyberSpace and the Use of Force* (Aegis Research Corporation 1999) 133.

[52] Jason Barkham, 'Information Warfare and International Law on the Use of Force' (2001) 34 *New York University Journal of International Law and Politics* 57, 80.

[53] Schmitt (n 38) 913. Jack Goldsmith has taken a similar approach, see Jack Goldsmith, 'How Cyber Changes the Laws of War' (2013) 24 *European Journal of International Law* 129, 133. See also Matthew Hoisington,

constitute a use of force where it 'results in a physical consequence, namely destruction of physical property, injury or loss of lives.'[54] Marco Roscini in turn maintains that the position is 'virtually uncontested'[55] that if a cyber attack causes physical damage to property or injury to persons then it would amount to a use of force.[56] 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.'[57] Daniel 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.'[58] Christopher Joyner and Catherine Lotrionte in turn find it 'persuasive' that cyber attacks which 'directly and intentionally result in non-combatant deaths and destruction' constitute uses of force.[59] 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'.[60] Like non-kinetic chemical and biological weapons, the use of which is considered to constitute a use of force especially due to their destructive effects to life and property;[61] cyber attacks, even despite their non-physical nature as weapons, can be similarly regarded as uses of force under Article 2(4) provided they have material effects.

Accordingly, the 'easy cases' for the use of force analysis in relation to cyber attacks, are those that have material effects similar to non-cyber uses of force. However, the more complex cases arise from those cyber attacks that do not directly cause visible physical harm,

---

'Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defense' (2009) 32 *Boston College International and Comparative Law Review* 439, 447.

[54] Dinniss (n 40) 74.

[55] Roscini (n 50) 53.

[56] ibid.

[57] Katharina Ziolkowski, 'Computer Network Operations and the Law of Armed Conflict' (2010) 49 *Military Law and the Law of War Review* 47, 70.

[58] Daniel B Silver, 'Computer Network Attack as a Use of Force under Article 2(4) of the United Nations Charter' (2002) 76 *International Law Studies Series US Naval War College* 73, 85.

[59] Christopher C Joyner and Catherine Lotrionte, 'Information Warfare as International Coercion: Elements of a Legal Framework' (2001) 12 *European Journal of International Law* 825, 850.

[60] Yoram Dinstein, 'Computer Network Attacks and Self-Defense' (2002) 76 *International Law Studies Series US Naval War College* 99, 103.

[61] Brownlie (n 37) 362.

such as injury to humans or damage to property. Non-material cyber attacks, such as where the operation of computer systems or networks is disrupted without destruction of hardware or only the integrity information is undermined, are difficult to characterise as uses of force.[62] For example, according to Dinniss, especially problematic are those instances '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.'[63] Barkham also recognises that those cyber attacks that only undermine the integrity of data, opposed to actually destroying it, would not be considered uses of force as there is no weapon involved nor property destroyed.[64] Roscini similarly highlights how it is a 'very difficult question to answer' whether the destruction of data can be equated to the destruction of physical property that would fall under Article 2(4).[65] William 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'.[66] He adopts the position taken by the authors of the Tallinn Manual, arguing that the data resident on a computer system can only be properly regarded as an object of an attack if it impacts on the functioning of the computer systems or networks to the degree that repairs are needed for them to re-operate again.[67]

Cyber attacks and non-intervention

In the literature on cyber attacks and the use of force, those measures not considered to cross the armed force threshold are generally considered as breaches of the non-intervention

[62] There is even debate as to whether severely disruptive cyber attacks against a state's critical infrastructure (without causing physical damage) would amount to a use of force. See Roscini (n 50) 55-61. This emphasis on material effects stands in contrast to how states regulate malicious cyber activities domestically. For example, under international law seeking to harmonise states' national cybercrime laws, states are required to criminalise unauthorised access by individuals (or corporations) to computer systems, and unauthorised data and system interference. However, these provisions only apply to non-state actors. See Convention on Cybercrime (Budapest, 23 November 2001) ETS 185, *entered into force* 1 July 2004, Articles 2, 4 and 5.
[63] Dinniss (n 40) 68.
[64] Barkham (n 52) 89.
[65] Roscini (n 50) 55.
[66] William H Boothby, 'Methods and Means of Cyber Warfare' (2013) 89 *International Law Studies Series US Naval War College* 387, 389.
[67] ibid 389-390.

principle instead. In non-cyber context, the non-intervention principle is a rule of international law according to which states cannot intervene in the domestic affairs of other states. The UN General Assembly's 1970 Declaration on Friendly Relations[68] describes it as the principle that:

> 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.[69]

As such, this principle also encompasses the non-use of force principle.[70] It prohibits states from intervening in another state's affairs in a way that seeks to coercively affect matters they are free to decide. These matters include a state's 'political, economic, social and cultural system' and the formulation of their own foreign policy.[71] Consequently, while the non-intervention principle encompasses the non-use of force principle, it is also broader in the sense that it also covers coercive 'non-forceful' measures. However, only a breach of the non-use of force principle (provided it rises to the level of an 'armed attack') can trigger a state's right to use force in self-defence, whereas simply breaching the non-intervention principle cannot.[72]

[68] GA Res. 2625 (XXV) of 24 October 1970.
[69] ibid.
[70] See *Military and Paramilitary Activities in and Against Nicaragua* (Nicaragua v United States), Judgment of 27 June 1986, ICJ Reports 1986, 14, para 205. See also *Armed Activities on the Territory of the Congo* (Democratic Republic of Congo v Uganda), Judgment of 19 December 2005, ICJ Reports 2005, 168, para 164.
[71] *Military and Paramilitary Activities in and Against Nicaragua* (n 70) para 205.
[72] Article 51 of the UN Charter recognises states' inherent right of self-defence when subject to an armed attack. According to the International Court of Justice, only the most 'grave' uses of forces can amount to an armed attack. *Military and Paramilitary Activities in and Against Nicaragua* (n 70) para 191. In contrast, however, measures below the use of force threshold only amounting to a breach of the non-intervention principle cannot trigger this right.

Compared to the volume of literature on cyber attacks and Article 2(4), few authors consider the non-intervention principle in relation to cyber attacks in-depth.[73] A notable exception is Russell Buchan who, focusing particularly on cyber attacks below the use of force threshold, argues that:

> 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.[74]

Nonetheless, most authors maintain that the principle is applicable. Among these authors, there is a general 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 non-material cyber attacks that do not easily fit with existing understandings of what constitutes armed force. 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.'[75] Roscini in turn 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.'[76] 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'.'[77] Similarly, Dinniss argues that cyber attacks with minimal effects or not manifesting in the physical sphere, but nonetheless warranting concern about

[73] Russell Buchan also notes that 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.' Russell Buchan, 'Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?' (2012) 17 *Journal of Conflict & Security Law* 211, 221.
[74] ibid 226.
[75] Marco Benatar, 'The Use of Cyber Force: Need for Legal Justification?' (2009) 1 *Goettingen Journal of International Law* 375, 395.
[76] Roscini (n 50) 115.
[77] ibid 65 citing GA Res. 2625 (XXV) of 24 October 1970.

whether they amount to force or not, will likely be considered as unlawful interferences instead.[78] 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 other states.'[79] Finally, the authors of the Tallinn Manual also took the view that 'cyber espionage and cyber exploitation operations' (low intensity cyber attacks) can amount to a breach of the non-intervention principle where they are coercive.[80] They give examples of measures below the use of force threshold involving the manipulation of data that could amount to breach of the non-intervention principle. These include 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.[81]

As such, the position reflected in the Tallinn Manual and adopted by most legal scholars is that cyber attacks generally require material effects – such as damage to property or injury to human beings – to constitute a use of 'force' pursuant to Article 2(4). The more problematic non-material cyber attacks that fall below this threshold are instead considered as potential breaches of the non-intervention principle alone. This is also illustrated in the existing analyses of the 2007 cyber attacks against Estonia in light of these principles.

The 2007 cyber attacks against Estonia

On the question of whether the cyber attacks against Estonia in 2007 constituted a breach of Article 2(4), the prevailing view holds that existing law would not extend to incident largely

[78] Dinniss (n 40) 74.
[79] Joyner and Lotrionte (n 59) 849.
[80] Schmitt (ed) (n 44) 44-45.
[81] ibid 45. For Schmitt's view on whether Russian actions during the 2016 US presidential election constituted a prohibited intervention, see Patrick Tucker, 'Did Russia's Election Meddling Break International Law? Experts Can't Agree' (*Government Executive*, 8 February 2017) <http://www.govexec.com/technology/2017/02/did-russias-election-meddling-break-international-law-experts-cant-agree/135260/> accessed 10 February 2017.

as no physical damage or injury to human beings was caused.[82] Illustrative of this position is 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.'[83] Therefore, he argues that 'in the absence of physical damage … the cyber attacks committed against Estonia cannot be regarded as an unlawful use of force for the purposes of Article 2(4).'[84]

Some also consider the criteria found in the commentary to the rules of the Tallinn Manual in relation to the attacks against Estonia. Nicholas Tsagourias questions whether under these criteria the incident would amount to a use of force, noting that:

> 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.[85]

Similarly, others adopt the view that even under the Tallinn Manual criteria, the Estonia incident would not amount to a use of force. Michael Gervais 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.'[86] As such, because these authors adopt the view that the incident would not be considered a use of force

[82] This article is not concerned with the attribution of state responsibility for the cyber attacks against Estonia. On cyber attacks and state responsibility generally, see for example Scott J Shackelford and Richard B Andres, 'State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem' (2011) 42 *Georgetown Journal of International Law* 971, 984-993.
[83] Buchan (n 73) 219.
[84] ibid.
[85] Nicholas Tsagourias, 'The Tallinn Manual on the International Law Applicable to Cyber Warfare: A Commentary on Chapter II - The Use of Force' in Terry D Gill (ed), *Yearbook of International Humanitarian Law Volume 15, 2012* (Volume 15, Springer 2014) 25.
[86] Michael Gervais, 'Cyber Attacks and the Laws of War' (2012) 30 *Berkeley Journal of International Law* 525, 540. Reese Nguyen 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 Reese Nguyen, 'Navigating Jus Ad Bellum in the Age of Cyber Warfare' (2013) 101 *California Law Review* 1079, 1123-1124.

under the Tallinn Manual criteria, it is implicit that they do not consider it to have crossed the use of force threshold under existing law.

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. 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 Solider.'[87] As such, he maintains that the cyber attacks constituted a violation of Estonia's sovereignty and breached the non-intervention principle.[88] 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.'[89] Similarly, Anders Henriksen maintains that while the incident did not reach a threshold triggering the right to self-defence,[90] if Russia was responsible and 'intended to coerce the Estonia politicians to undo their decision to remove the war memorial' then it would amount to a breach of the non-intervention principle.[91] Consequently, because the cyber attacks, despite their duration and disruptiveness, 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.

As is evident from the legal analyses of cyber attacks and the threshold distinction between the non-use of force and non-intervention principles, and from the application of

[87] Buchan (n 73) 226.
[88] ibid.
[89] Tsagourias (n 85) 35.
[90] Anders Henriksen, 'Lawful State Responses to Low-Level Cyber-Attacks' (2015) 84 *Nordic Journal of International Law* 323, 327.
[91] ibid 340.

these principles to the Estonia incident, the law embodies a limited view of violence. The notion of force within Article 2(4) requires some form of physical violence, whether inflicted through the use of kinetic weapons or non-kinetic weapons causing damage or destruction of material objects or injury or death to human beings. This conception of violence also underpins existing accounts of when cyber attacks amount to a use of force, and the dominant position is that they will only do so where they have material effects resembling those of conventional uses of force. The Tallinn Manual also cements this idea that without some form of physical damage to computer hardware at least, cyber attacks cannot amount to a use of force.[92] This means that where a cyber attack falls below this threshold, it is only considered as a potential breach of the non-intervention principle and effectively conceptualised as a form of non-violence outside the ambit of Article 2(4). As such, existing law lacks the ability to adequately recognise the harm caused by cyber attacks with non-material effects, such as those against Estonia. This is evident in the prevailing view that the incident would not constitute a use of force and only constitute a breach of the non-intervention principle provided Estonia was coerced into changing its policy in regards to the location of the war memorial statue.

The ontological constraints of Article 2(4)

It is argued that the law's fixation on physical damage highlights its ontologically constrained view of violence – the law is only capable of recognising physical damage to material objects or human beings within its existing conception of violence.[93] Disrupting the operation of non-

[92] See Schmitt (ed) (n 44) 48. Further, in discussing the notion of 'cyber attack' in the international humanitarian law context (and therefore not directly in relation to the use of force), the authors note how 'acts of violence' are generally those releasing kinetic force, with the exception of non-kinetic 'chemical, biological, or radiological' means also constituting attacks. They maintain that the crux lies in the effects caused and 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.' ibid 106-107.

[93] Jackson Maogoto makes a similar point, arguing that there is uncertainty in the assessments of when a cyber attack constitutes a use of force 'since the baseline is that the *UN Charter* is by and large fixated on unlawful

material entities or processes such as websites and networks does not amount to form of damage or harm that the law is capable of recognising. Accordingly, the attacks against Estonia cannot amount to a use of force primarily because their effects did not subscribe to the law's anthropocentric and materialist conception of violence. Similar limitations are also recognised by authors like Schmitt and Sheng Li who seek to make arguments for how the cyber attacks against Estonia could be considered a use of force. Schmitt for example notes that, while under existing law the cyber attacks against Estonia would not amount to a use of force, the law is likely to develop into the direction that it would.[94] Drawing on the factors that later formed the basis for the Tallinn Manual criteria, he writes in relation to 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.'[95] According to Schmitt, this was evident in the severe disruption of government functions and services, and the negative effects on the economy and daily life of Estonian people.[96] Li in turn likens the cyber attacks to an information blockade that, like a naval blockade, should constitute a use of force as it threatened the welfare of a state and its people that were 'heavily dependent upon access to digital information for their physical and material well-being.'[97] 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. For Schmitt the cyber attacks had a fundamental impact on the functioning of Estonian society as governmental functions, services, and the daily lives of Estonia people. For Li in turn, the cyber attacks resulted in an informational blockade that impacted on the material wellbeing of Estonians.

---

violence threatened or committed against persons and/or property.' Jackson Nyamuya Maogoto, *Technology and the Law on the Use of Force* (Routledge 2015) 64.

[94] Michael N Schmitt, 'Cyber Operations and the Jus Ad Bellum Revisited' (2011) 56 *Villanova Law Review* 569, 605.

[95] ibid 577.

[96] ibid.

[97] Li (n 14) 196.

Despite these arguments about how existing law could be extended to the incident, the prevailing position is that the attacks did not amount to a use of force under existing law largely due to a lack of physical damage. As a result this ontologically constrained view of violence, 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. Further, given the tendency to consider these types of attacks as only potential breaches of the non-intervention principle, non-destructive cyber attacks are likened to a form of non-violence outside Article 2(4)'s scope. However, as the Estonia incident demonstrated, even cyber attacks without material effects are capable of disrupting the functioning of states increasingly dependent on information and communication technologies (ICTs) and harming the states in new ways that should be recognised by the law. As the next section will demonstrate, disruptive or non-material cyber attacks can be considered a form of 'informational violence' against the state that is increasingly capable of harming the state by undermining its proper functioning.

II An informational approach

This section develops an informational approach to the Estonia incident as a means of overcoming the limited conception of violence evident in existing law. It first provides an overview of Luciano Floridi's 'information ethics'[98] which offers an alternative ontology. Through its conceptual framework, both the material and non-material effects of cyber

[98] Floridi's information ethics was originally developed in Luciano Floridi, 'Information Ethics: on the Philosophical Foundation of Computer Ethics' (1999) 1 *Ethics and Information Technology* 33 and most recently and comprehensively in Luciano Floridi, *The Ethics of Information* (Oxford University Press 2013). On information ethics and cyber warfare, see Mariarosaria Taddeo, 'Information Warfare: A Philosophical Perspective' (2012) 25 *Philosophy & Technology* 105; Mariarosaria Taddeo, 'Just Information Warfare' (2016) 35 *Topoi* 213; Ugo Pagallo, 'Cyber Force and the Role of Sovereign States in Informational Warfare' (2015) 28 *Philosophy & Technology* 407; Massimo Durante, 'Violence, Just Cyber War and Information' (2015) 28 *Philosophy & Technology* 369. See also Massimo Durante, 'Re-designing the Role of Law in the Information Society: Mediating between the Real and the Virtual' (2010) 2 *European Journal of Legal Studies* 19; Massimo Durante, 'Dealing with Legal Conflicts in the Information Society. An Informational Understanding of Balancing Competing Interests' (2013) 26 *Philosophy & Technology* 437; Ugo Pagallo, 'The Realignment of the Sources of the Law and their Meaning in an Information Society' (2015) 28 *Philosophy & Technology* 57.

attacks can be considered on all entities and environments, whether natural or artificial, physical or virtual. As such, it offers a way through which the non-material harm caused by the attacks can be taken seriously.[99]

Information ethics – an overview

Floridi's information ethics is best described as a form of environmental ethics that extends its ethical concern beyond the physical environment to also digital environments and entities. 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.[100] 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.[101]

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'.[102] For methodological purposes information ethics advocates the adoption of an informational ontology which provides a minimum common denominator through which all entities can be seen in similar terms.[103] As such, by adopting a

[99] Floridi's information ethics provides a conceptual framework that seeks to address the ethical challenges associated with ICTs. Given that it incorporates all entities into its ethical discourse as information entities (and not simply computers or data), it is uniquely suited for considering issues surrounding cyber warfare and hybrid warfare. It allows for consideration of the entities (whether human beings, robots or computer viruses) involved in warfare, the environments (whether real or virtual) in which it is waged, and the various forms of violence associated with warfare (whether material or non-material). See Taddeo (n 98) 216. As such, an informational approach offers a means through which the law can be updated to overcome its ontological constraints.
[100] Luciano Floridi, *Information: A Very Short Introduction* (Oxford University Press 2010) 111.
[101] ibid 112.
[102] Floridi (n 98) 44. See also Floridi (n 98) 6; Luciano Floridi, *The Fourth Revolution* (Oxford University Press 2014) 41.
[103] Luciano Floridi, 'Information Ethics, its Nature and Scope' (2006) 36 *Computers and Society* 21, 33.

perspective from which all entities can be viewed in terms of their information structures, all entities can be seen as information entities.[104] 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.[105] Further, information ethics adopts the view that everything, by virtue of its existence, should have a basic degree of moral value. This is the principle of ontological equality.[106]

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 develop in a way which is appropriate to its nature.'[107] 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.[108]

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.[109] 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.[110]

---

[104] ibid.
[105] Floridi (n 98) 113.
[106] Floridi (n 98) 44.
[107] Floridi (n 98) 113.
[108] Floridi (n 98) 67.
[109] ibid 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 (n 98) 221-222; Pagallo (n 98) 416-419.
[110] Luciano Floridi, 'Information Ethics: An Environmental Approach to the Digital Divide' (2002) 9 *Philosophy in the Contemporary World* 39, 42.

The state entity

Drawing on this conceptual framework, both the harm that cyber attacks cause and the state as an entity subject to harm can be reconceptualised. Viewed informationally, the state entity can be seen as a non-static and continuously changing entity. Given the nature of global information infrastructures and information flows, it 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 a state, and government communications with foreign governments and regional and international organisations – various information flows continuously move in and out of this entity. This entity also has a trajectory towards complexity as the amount of global information flows, devices, and users increase over time.[111] Therefore, the informational substance of the state as a dynamic or non-static entity continuously changes, however, its form or pattern as an information entity persists.

The pattern or form of the state entity is evident in its systematic features. Floridi for example, drawing on the use of the term in computer science, describes the state as a 'multiagent system'.[112] It is an entity capable of interaction, it has a degree of autonomy, it is adaptable, and it has an inherent purpose towards which it gears its functions.[113] As an

[111] The projected number of mobile devices by 2020 is 11.6 billion which equates to 1.5 mobile devices per capita. CISCO, 'Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2015–2020' (3 February 2016) <http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.pdf> accessed 15 November 2016. Similarly, with the Internet of Things, more objects are becoming embedded with ICTs and capable of communicating and interacting. See Luigi Atzori, Antonio Iera and Giacomo Morabito, 'The Internet of Things: A Survey' (2010) 54 *Computer Networks* 2787, 2787. Further, the notion of 'Big Data' seeks to capture the explosion in the amount of global data that is increasingly 'captured, communicated, aggregated, stored, and analyzed' and increasingly essential to modern economic activity. James Manyika and others, *Big Data: The Next Frontier for Innovation, Competition, and Productivity* (McKinsey Global Institute, May 2011) <http://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Big%20data%20The%20next%20frontier%20for%20innovation/MGI_big_data_full_report.ashx> accessed 15 November 2016, iv.

[112] Floridi (n 102) 180-181.

[113] Floridi attributes the state (and other multiagent systems, such as international organisations) with these features describing them as teleological, interactive, autonomous, and adaptable. ibid. 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

information system, the state entity is situated not only in the physical world (within its territory), but also in the virtual world of cyberspace in which it increasingly interacts with other entities. In other words it 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 physical ICT infrastructure within its territory, but also to its conduct of 'ICT-related activities'.[114] 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 its various components as well as externally with other entities (such as other state entities, international organisations, and multinational corporations). In some cases it constitutes a component or sub-system within these larger systems (for example, in regional or international organisations). 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.[115]

---

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 (n 29) 307-309. Consequently Wendt goes on to describe states as superorganisms, see ibid 309-310.

[114] Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN Doc A/68/98, 24 January 2013) para 20.

[115] On the features of a multiagent system in computer science, see Michael Wooldridge, *An Introduction to Multiagent Systems* (John Wiley & Sons 2002) 3.

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 its structure as an entity. These structures that make up the information system are 'bound together by a system of communication',[116] both internally within and between these structures, and externally between its institutions and those of other state entities.[117] 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.[118] 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

[116] Norbert Wiener, *Cybernetics: or Control and Communication in the Animal and the Machine* (Technology Press 1948) 33 cited in Terrell Ward Bynum, 'Norbert Wiener and the Rise of Information Ethics' in Jeroen Van Den Hoven and John Weckert (eds), *Information Technology and Moral Philosophy* (Cambridge University Press 2008) 12.

[117] 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.' Anne-Marie Slaughter, *A New World Order* (Princeton University Press 2005) 5.

[118] 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 (n 116) 12 (emphasis in original).

and enable it to operate as a coherent and autonomous system.[119] 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 (government 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 the information system (criminal law, civil law). A range of protocols also govern the interactions of the information system as a whole with other information systems (public international law). Therefore, the information structures by which the state entity as an information system is constituted, are bound together by numerous protocols which give the system a degree of coherence over time and delineate it as an entity separate from other entities.

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 information system is to care for and protect the wellbeing of its region of the infosphere.[120] Consequently, the essence of the state entity is to care for and protect the entities and environments in which it is situated. This includes the natural

[119] 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 Timothy Colburn and Gary Shute, 'Abstraction, Law, and Freedom in Computer Science' (2010) 41 *Metaphilosophy* 345, 346. Lawrence Lessig famously argued that 'code is law' – that is, the computer code is central to regulating behaviour in cyberspace. Lawrence Lessig, *Code Version 2.0* (Basic Books 2006) 5.

[120] The notion of an entity's 'region of the infosphere' is drawn from Floridi's informational analysis of business. See Floridi (n 98) 289-290.

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.[121] 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. The purpose of the state entity is therefore to protect these entities from entropy, and care for the environments in which they exist.

Informational violence

Against this image of the state entity as an information system, the harm inflicted by cyber attacks can be rethought in terms of entropy. Others have also sought to reconsider the harm in cyber attacks. Randall Dipert for instance suggests an ontological rethinking of the harm caused by cyber attacks and 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.'[122] 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

[121] Similarly, Nazli Choucri notes that against the conventional way of thinking about national security in terms of protecting borders, in the twenty-first century '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.' Nazli Choucri, *Cyberpolitics in International Relations* (The MIT Press 2012) 38.
[122] Randall R Dipert, 'The Ethics of Cyberwarfare' (2010) 9 *Journal of Military Ethics* 384, 386 (emphasis in original).

an economy) is in some way impaired or degraded.'[123] Massimo Durante also considers the notion of violence specifically from an information ethics perspective. He makes a distinction between informational and physical violence arguing that physical violence arises 'when a disruptive activity damages, deteriorates, deletes or suppresses an informational object.'[124] Essentially, where the entropy that is caused physically (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 depriving an information entity of the capacity of being *that* source of information that it is.[125] He maintains 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.[126] According to him, it is a form of 'radical regardlessness' towards an entity.[127]

The informational reconceptualisation of violence that is 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. Additionally, however, the focus here is on how cyber attacks undermine the integrity of state entities, both in terms of how they actually disrupt or damage computer systems or their operation within states, as well as how this can be seen to harm the state entity as an information system on a more conceptual level.

Accordingly, drawing on the principle of ontological equality which provides that all entities have a basic right to exist and flourish in a way that is appropriate to their nature, the harm to an entity can be understood through the concept of entropy – that is, as some form of

[123] ibid 397.
[124] Durante (n 98) 383 (emphasis in original).
[125] ibid 382-383.
[126] ibid 383.
[127] ibid.

damage, destruction, degradation, corruption or pollution of an entity, impacting on its very being and right to exist.[128] While 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',[129] 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.[130] However, it is argued here that pursuant to the ontological equality principle, all things should have value in themselves, and because of this any entity is capable of being 'harmed' even if it has no direct connection to human interests.[131] Harm in this context is to the entity's existence and right to flourish – and consequently to its interest in flourishing according to its nature. As such, increases in entropy can be seen as harm to an entity without any necessary connection to human interests in objects or information entities. The harm, in the form of damage or degradation of an entity, is intrinsically connected to its inherent interest in its existence and right to flourish pursuant to the ontological equality principle.[132]

Consequently, the harm caused by the 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 the state entity's ability to interact, its autonomy, the protocols according to which it operates,

[128] As Floridi writes, it is an 'impoverishment of *Being*.' Floridi (n 98) 67 (emphasis in original).
[129] 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 ontocentric, more neutral term, with 'annihilation' as the level of most severe damage or highest degree of metaphysical entropy.' ibid 182.
[130] Joel Feinberg considers the various ways in which the extended notion of harm can be used, for instance, that '[b]y smashing windows, vandals are said to harm people's property; neglect can harm one's garden; frost does harm to crops.' Joel Feinberg, *Harm to Others* (Oxford University Press 1984) 32. Similarly, 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. ibid 33.
[131] 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.' ibid.
[132] 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. See Floridi (n 98) 71-72.

and the very essence of the state entity as an information system – 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. As such, a reconceptualisation of the state as an entity subject to violence and of the notion of violence offers a means through which both material and non-material cyber attacks can be seen as capable of harming the state entity.

An informational approach to the 2007 cyber attacks against Estonia

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,[133] there is a growing number of Internet users,[134] 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.[135] 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.[136] Similarly, there are continuous capital flows in and out of its economy.[137] In addition to these information flows, when viewed informationally, all potential entities can be

[133] International Telecommunication Union, 'Measuring the Information Society Report' (2015) <http://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2015/MISR2015-w5.pdf> accessed 15 November 2016.
[134] 'Internet users (per 100 people)' (*The World Bank*) http://data.worldbank.org/indicator/IT.NET.USER.P2 accessed 15 December 2016.
[135] The International Telecommunication Union'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 (n 133) 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). ibid 39-41. In 2015 Estonia's IDI was 8.05 (the highest being the Republic of Korea with 8.93) ranking it 20th in the world. See ibid 46.
[136] World Economic Forum, 'The Global Technology Report' (2015) <http://reports.weforum.org/global-information-technology-report-2015> accessed 15 November 2016.
[137] 'Economy in Numbers' (*Estonia.eu*, 20 April 2016) <http://estonia.eu/about-estonia/economy-a-it/economy-in-numbers.html> accessed 15 December 2016.

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. 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 European Union (EU) and the North Atlantic Treaty Organisation (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 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.[138] 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.[139] The relationship between Estonians and the government became one integrated with ICTs – by verifying their digital identities with electronic 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.'[140] 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

[138] Republic of Estonia Ministry of Economic Affairs and Communications, 'Information Society Strategy 2013' (2006) <http://unpan1.un.org/intradoc/groups/public/documents/unpan/unpan033997.pdf> accessed 15 November 2016, 5-6.

[139] On a range of 'components' of Estonia's digital society, ranging from e-government, e-health and e-education initiatives in Estonia, see 'Components for Digital Society' (*e-Estonia.com*) <https://e-estonia.com/components> accessed 15 December 2016.

[140] See 'X-Road' (*e-Estonia.com*) <https://e-estonia.com/component/x-road https://e-estonia.com/components> accessed 15 December 2016; 'Electronic ID Card' (*e-Estonia.com*) <https://e-estonia.com/component/electronic-id-card> accessed 15 December 2016.

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 information system 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.

Entropy caused by the cyber attacks

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 the 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.

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.[141] 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.[142] 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, and 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.[143] The properties of these entities had been corrupted, meaning they were able to be used as slaves to cause significant

[141] 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, Kaska and Vihul (n 5) 21.
[142] ibid 24.
[143] Landler and Markoff (n 2).

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.[144] When used in the DDoS attack, the information requests that were sent by this collective of corrupted computers, unlike the legitimate requests that 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, sought to disrupt the functioning of the Estonian entity's information infrastructure. 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.[145] 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

[144] A 'botnet' is a network of synchronised bots (a network of robots) performing the commands of their controllers. Jelena Mirkovic and others, *Internet Denial of Service: Attack and Defense Mechanisms* (Prentice Hall Professional Technical Reference 2005) 291.

[145] From the information available on the volume of data used in the attacks against Estonia, most were either less than ten megabits per second (Mbps) or between ten Mbps and thirty Mbps and lasted less than an hour. However, some of the attacks were made up of a significantly larger amount of data, reaching over ninety Mbps and lasting more than ten hours. See Nazario (n 6).

from functioning properly.[146] 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. For example, the DDoS attacks on 1 May that resulted in ISPs needing to reboot their systems, while only for twenty seconds,[147] disrupted the functioning of a range of computer systems and the services they provided access to, and 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 one and a half hours on each occasion.[148] 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.[149] Even though some of these attacks were short in duration, together they resulted in a sustained attack against government networks.[150] For example, the Estonian Parliament's email service was down for twelve hours as a result of the attacks.[151] Similarly, the attacks disrupted the online availability of public services, particularly for Estonians overseas.[152]

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

[146] Tikk, Kaska and Vihul (n 5) 21-22.
[147] Finn (n 7).
[148] Tikk, Kaska and Vihul (n 5) 20.
[149] Nazario (n 6).
[150] ibid.
[151] Finn (n 7).
[152] Tikk, Kaska and Vihul (n 5) 25.

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.[153] 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.[154] 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[155] or public services.[156] 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

[153] These are among the measures taken by Estonia's Computer Emergency Response Team (CERT), see ibid 24.
[154] ibid 24.
[155] Landler and Markoff (n 2).
[156] Tikk, Kaska and Vihul (n 5) 25.

undermine the ability of the DDoS attacks to cause further increases in entropy within the Estonian entity. 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. This in turn also demonstrated its adaptability as an information system.

Conclusion

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. The Estonian entity can be seen as a dynamic but systematic entity that is constituted by information structures and protocols, located within a particular 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 ability to interact, its autonomy, and its capacity to care for and protect its region of the infosphere. As such, they constituted a form of informational violence against the Estonian entity, despite the lack of material damage to physical objects or injury to human beings.

This is in contrast to how existing law on the use of force conceptualises violence which, as demonstrated above, is limited to recognising only forms of physical violence as manifested in uses 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 attacked through 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 more easily be considered 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. However, making this distinction primarily on whether or not the attack in question results in material effects is artificial.[157] As one of the central purposes of the UN Charter based legal order is the containment of interstate violence and conflict,[158] 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.

Consequently, an informational approach offers a means to overcome the law's ontological constraints rendering 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

[157] 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 (n 14) 214.
[158] UN Charter, Preamble and Article 2(3). See also Cassese (n 31) 40.

violence, as evident in the depiction of such attacks as a form of non-violence below the use of force threshold. Therefore, by adopting an informational approach, a broader ontological spectrum of violence can be recognised and cyber attacks such as those against Estonia can be seen as a form of informational violence against the essence of the state as an entity.