GRIFFITH UNIVERSITY

Stuxnet and international law on the use of force: an informational approach

Author

Haataja, Samuli, Akhtar-Khavari, Afshin

Published

2018

Journal Title

Cambridge International Law Journal

Version

Accepted Manuscript (AM)

DOI

10.4337/cilj.2018.01.05

Rights statement

© Samuli Haataja and Afshin Akhtar-Khavari, 2018. This is the author-manuscript version of this paper. The definitive, peer reviewed and edited version of this article is published in Leadership and the Humanities, Volume: 7 Issue: 1, Pages:99–121, 2018.

Downloaded from

http://hdl.handle.net/10072/390000

Griffith Research Online

https://research-repository.griffith.edu.au

Stuxnet and International Law on the Use of Force: an Informational Approach*

Samuli Haataja
Griffith University

Afshin Akhtar-Khavari
Queensland University of Technology

This article considers the Stuxnet cyberattack in the context of international law on the use of force below the armed attack threshold. With a focus on the concept of 'force' within Article 2(4) of the UN Charter, it is argued that international law embodies an anthropocentric and materialist view of violence. Violence, as traditionally understood in the context of Article 2(4), involves a state using kinetic weapons to damage or destroy physical property, or injure or kill human beings within another state. Using the Stuxnet incident as a case study and as a tool of critique, it is argued that the law's one-dimensional conception of violence that focuses on physical damage limits its ability to recognise the non-material harm Stuxnet caused to countless virtual entities and processes. As such, the law does not adequately account for the non-material ways in which states that are increasingly dependent on information and communication technologies (ICTs) can be harmed. As a means of overcoming the law's limited conception of violence, this article draws on Luciano Floridi's information ethics. This is a theory that extends its ethical concern beyond the material world to include all entities, whether natural or artificial, physical or virtual. In this article it is used both to critique the law's anthropocentrism and materialism and to provide an alternative account of the harm that Stuxnet caused.

Keywords: use of force, Stuxnet, information ethics

1 INTRODUCTION

Malevolent state activities in and through cyberspace have been a growing concern in recent years.[1] Well-known incidents include the large scale Distributed Denial of Service (DDoS) attacks against Estonia in 2007 in response to its government's decision to relocate a politically contentious war memorial statue, and the 2008 cyberattacks against Georgia during the armed conflict over the South Ossetia region.[2] More recent examples include the 2015 incident in which the personal data of approximately 21.5 million United States (US) federal employees was compromised by a 'Chinese espionage operation',[3] and unauthorised access by Russian intelligence agencies to the computer systems of the US Democratic Party during the 2016 presidential election.[4] These incidents were either conducted by state actors or are believed to have been conducted with some degree of state approval, and all involved some form of attack

* The authors would like to thank the following colleagues for their input into this paper: Associate Professor Kieran Tranter, Professor Tim McCormack and Professor Ugo Pagallo. We also wish to thank the two anonymous reviewers of this article for their feedback and helpful suggestions.

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

[2] Ian Traynor, 'Russia accused of unleashing cyberwar to disable Estonia' *The Guardian* (London, 17 May 2007) <www.theguardian.com/world/2007/may/17/topstories3.russia> accessed 15 November 2016; John Markoff, 'Before the Gunfire, Cyberattacks' *The New York Times* (New York, 12 August 2008) <www.nytimes.com/2008/08/13/technology/13cyber.html> accessed 15 November 2016.

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

[4] 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) <www.nytimes.com/2016/07/30/us/politics/clinton-campaign-hacked-russians.html?_r=2> accessed 15 November 2016.

against government websites or networks, agencies or affiliated institutions. The degrees of harm or damage caused by these incidents also vary. While the Estonia and Georgia incidents involved DDoS attacks designed to disrupt the operation of computers and networks, the latter incidents mainly involved information or data being compromised. As such, a common feature of all of these incidents is that the primary effect of the cyberattacks was the disruption of the operation of websites or networks (virtual entities and processes) or the undermining of the integrity of information.[5] None of these incidents involved cyberattacks causing direct and immediate damage to physical property or injury to human beings.

In contrast to these non-destructive or non-material cyberattacks, in 2010 the first known example of states using cyber means to cause physical damage in another state became public. Dubbed 'Stuxnet', a sophisticated piece of malicious software was discovered in 2010. It is believed to have been created by the US and Israel with the aim of undermining Iran's ability to enrich uranium at its enrichment facility in Natanz. It was a technically sophisticated 'cyber weapon' designed to infect non-networked computers within the Natanz facility in order to adjust the frequency setting that determines the speed at which nuclear centrifuges are spun. It used a number of features to prevent anti-virus and other security mechanisms from detecting it, and also made it appear to the human operators of the facility that the infected computers were operating normally. Ultimately, it is believed to have been responsible for causing physical damage to approximately 1000 centrifuges.

This article considers the Stuxnet cyberattack in the context of international law on the use of force below the armed attack threshold. With a focus on the concept of 'force' within Article 2(4) of the UN Charter, it is argued that international law embodies an anthropocentric and materialist view of violence. Violence, as traditionally understood in the context of Article 2(4), involves a state using kinetic weapons to damage or destroy physical property, or injure or kill human beings within another state. Using the Stuxnet incident as a case study and as a tool of critique, it is argued that the law's one-dimensional conception of violence that focuses on physical damage limits its ability to recognise the non-material harm Stuxnet caused to countless virtual entities and processes in disrupting the operation of the Natanz facility. As such, the law does not adequately account for the non-material ways in which states that are increasingly dependent on information and communication technologies (ICTs) can be harmed. As a means of overcoming the law's limited conception of violence, this article draws on Luciano Floridi's information ethics. This is a theory that extends its ethical concern beyond the material world to include all entities, whether natural or artificial, physical or virtual. In this article it is used both to critique the law's anthropocentrism and materialism and to provide a more accurate account of the harm that Stuxnet caused.

This article is divided into three parts. The first part provides an overview of Stuxnet, who is believed to be responsible for it, and its impact on the uranium enrichment facility in Natanz, Iran. The second part examines the conception of violence that underpins the orthodox understanding of the notion of 'force' within Article 2(4), and how the prohibition on the use of force is thought to apply to cyberattacks and specifically to the Stuxnet incident. Finally, the third part gives an overview of information ethics and develops an informational approach to the Stuxnet incident.

2 STUXNET

Stuxnet was first discovered in June 2010 by a Belarussian internet security firm working for a client in Iran.[6] It was described as a 'turning point' in the design and purpose of malicious

[5] Cyberattacks are commonly defined as referring to deliberate computer enabled actions used 'to alter, disrupt, deceive, degrade, or destroy adversary computer systems or networks or the information and/or programs resident in or transiting these systems or networks.' William Owens, Kenneth Dam, and Herbert Lin (eds), *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities* (The National Academies Press, Washington DC 2009) 10-11.

[6] Josh Halliday and Julian Borger, 'Nuclear plants likely target of foiled cyber sabotage' *The Guardian* (London, 25 September 2010) <www.theguardian.com/world/2010/sep/25/iran-cyber-hacking-nuclear-plants> accessed 15 November 2016.

software.[7] Unlike other computer viruses or worms that are commonly designed for financial gain, for instance, Stuxnet was specifically designed for sabotage.[8] It appeared that it was tailored to target the computer systems used to control important infrastructure, as the hardware and software configurations it targeted were those used to operate a range of industrial equipment found in power grids, power plants, pipelines and dams.[9] While it had spread to over 100,000 computers around the world, 60% of these were located in Iran.[10]

The exact purpose of Stuxnet and who was responsible for its creation were not known when it was first discovered in June 2010. However, given its technical sophistication, it was widely believed that a group of hackers could not have been able to create it, and that instead, a nation-state was responsible for its development.[11] Stuxnet's design for example showed that its creation required a sophisticated team of programmers and an organisation with 'substantial financial resources to develop, test and then release such a program'.[12]

In September 2010 there was already some speculation that the enrichment facility at Natanz was the target of the attacks.[13] In November 2010, only days after computer security company Symantec released information they had discovered in the process of reverse engineering Stuxnet—namely, that it targeted specific frequency converter drives operating in a very particular way—reports from the International Atomic Energy Agency (IAEA) noted that Iran had 'stopped feeding hot uranium gas into its thousands of centrifuges'.[14] As Iranian officials did not provide any reason for this, it led some to believe that it was the result of the operators of the Natanz facility disconnecting computers and restoring systems to ensure that all traces of Stuxnet were removed.[15] Further, in late December 2010, the Institute for Science and International Security released a report in which it had compiled data from the IAEA's quarterly reports on Iran.[16] The IAEA monitors Iran's implementation of the *Treaty on the Non-Proliferation of Nuclear Weapons*[17] pursuant to the safeguard agreements that non-nuclear weapon states such as Iran have with the IAEA.[18] As such, the IAEA has surveillance cameras monitoring the perimeter of the centrifuge cascade area (but not the area itself).[19] It was reported that in the six-month period following late 2009, the footage showed that Iran had 'dismantled more than 10 percent of

---

[7] Dylan Welch, 'Cyber soldiers' *The Sydney Morning Herald* (Sydney, 9 October 2010) <www.smh.com.au/technology/technology-news/cyber-soldiers-20101008-16c7e> accessed 15 November 2016.

[8] Halliday and Borger (n 6).

[9] Riva Richmond, 'Malware Hits Computerized Industrial Equipment' *The New York Times* (New York, 24 September 2010) <https://bits.blogs.nytimes.com/2010/09/24/malware-hits-computerized-industrial-equipment/> accessed 15 November 2016; John Markoff, 'A Code for Chaos' *The New York Times* (New York, 2 October 2010) <www.nytimes.com/2010/10/03/weekinreview/03markoff.html> accessed 15 November 2016.

[10] Nicolas Falliere, Liam O Murchu and Eric Chien, 'W32.Stuxnet Dossier. Version 1.4' (Symantec 2011) < www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf> 5–6, accessed 11 February 2018.

[11] Richmond (n 9).

[12] Markoff (n 9).

[13] John Markoff and David Sanger, 'In a Computer Worm, a Possible Biblical Clue' *The New York Times* (New York, 29 September 2010) <www.nytimes.com/2010/09/30/world/middleeast/30worm.html?scp=2&sq=stuxnet&st=cse> accessed 15 November 2016.

[14] Falliere, Murchu, and Chien (n 10); Glenn Kessler, 'Centrifuges in Iran were shut down, IAEA report says' *The Washington Post* (Washington DC, 24 November 2010) <www.washingtonpost.com/wp-dyn/content/article/2010/11/23/AR2010112306964.html> accessed 15 November 2016.

[15] Kim Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon* (Crown, New York 2014) 237–238.

[16] David Albright, Paul Brannan and Christina Walrond, 'Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? Preliminary Assessment' (Institute for Science and International Security, 2010) <http://isis-online.org/isis-reports/detail/did-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant> accessed 15 November 2016.

[17] Treaty on the Non-Proliferation of Nuclear Weapons (adopted 1 July 1968, entered into force 5 March 1970) 729 UNTS 161.

[18] N Jansen Calamita, 'Sanctions, Countermeasures, and the Iranian Nuclear Issue' (2009) 42 Vanderbilt Journal of Transnational Law 1393, 1399–1400.

[19] David Albright, Paul Brannan and Christina Walrond, 'Stuxnet Malware and Natanz: Update of ISIS December 22, 2010 Report' (Institute for Science and International Security, 2011) 3 <http://isis-online.org/isis-reports/detail/stuxnet-malware-and-natanz-update-of-isis-december-22-2010-reportsupa-href1/8> accessed 15 November 2016.

the Natanz plant's 9,000 centrifuge machines used to enrich uranium'.[20] As such, an estimated 900–1000 centrifuges were reported to have broken.[21]

In January 2011, the New York Times reported that Stuxnet was a joint US and Israeli effort targeted at the Natanz facility.[22] The following year, in June 2012, the New York Times reported that the name of this operation was 'Olympic Games'.[23] Interviews with current and former US, European and Israeli officials revealed that Stuxnet was part of this operation which originally started during President George W. Bush's administration and later intensified under President Barack Obama's administration. It had involved an extensive development programme and had to be tested at what was described as a 'virtual replica of Natanz'.[24] According to these reports, given that Stuxnet needed to be physically introduced into the Natanz facility (that is, it could not be relayed via the internet), they relied on engineers and maintenance workers with physical access to the facility, for example, to unknowingly infect the computers therein.[25] USB thumb drives were reported to have been 'critical in spreading the first variants of the computer worm', while more sophisticated methods were used to further spread and deliver the code to the computers it targeted.[26] Originally, Stuxnet was not meant to spread outside the computers at the Natanz facility, and this was attributed to an error in its code which was reported to likely have been a later modification by the Israelis.[27]

Iran has not confirmed that Stuxnet was the cause of broken centrifuges at Natanz. However, Iranian officials have confirmed that some of their computers were infected by a computer virus. For instance, in September 2010 an Iranian official admitted that a computer 'worm had infected more than 30,000 computers, including personal computers owned by employees of the nuclear power plant near Bushehr'.[28] Also, according to reports in November 2010, Iran's President, Mahmoud Ahmadinejad, maintained that Iran's enemies 'had been successful in making problems for a limited number of our centrifuges, with software they had installed in electronic devices'.[29] When asked specifically about Stuxnet and whether it had been responsible, President Ahmadinejad responded with silence.[30] Further, around the same time, Iran's Vice President, Ali Akbar Salehi, who is also the head of the Iranian Atomic Energy Organisation, maintained that '[o]ne year and several months ago, Westerners sent a virus to [our] country's nuclear sites', but that the virus was discovered and prevented from causing harm to Iran's progress in the nuclear field.[31] Accordingly, while Iran has not admitted that Stuxnet caused damage to its nuclear centrifuges, it has acknowledged having issues with a computer virus. The timeframe referred to, especially in the Vice President's remarks, corresponds to the time at which, according to IAEA reports, there was a decline in the number of operational centrifuges.

---

[20] Joby Warrick, 'Iran's Natanz nuclear facility recovered quickly from Stuxnet cyberattack' *The Washington Post* (Washington DC, 16 February 2011) <www.washingtonpost.com/wp-dyn/content/article/2011/02/15/AR2011021506501.html> accessed 15 November 2016.

[21] Ibid.

[22] William Broad, John Markoff and David Sanger, 'Israeli Test on Worm Called Crucial in Iran Nuclear Delay' *The New York Times* (New York, 15 January 2011) <www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html> accessed 15 November 2016.

[23] David Sanger, 'Obama Order Sped Up Wave Of Cyberattacks Against Iran' *The New York Times* (New York, 1 June 2012) <www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html> accessed 15 November 2016.

[24] Ibid.

[25] Ibid.

[26] Ibid.

[27] Ibid.

[28] David Sanger, 'Iran Fights Malware Attacking Computers' *The New York Times* (New York, 25 September 2010) <www.nytimes.com/2010/09/26/world/middleeast/26iran.html> accessed 15 November 2016; Thomas Erdbrink and Ellen Nakashima, 'Iran struggling to contain 'foreign-made' computer worm' *The Washington Post* (Washington DC, 28 September 2010) <www.washingtonpost.com/wp-dyn/content/article/2010/09/27/AR2010092706606.html> accessed 15 November 2016.

[29] Thomas Erdbrink, 'Ahmadinejad: Iran's nuclear program hit by sabotage' *Washington Post* (Washington, 29 November 2010) <www.washingtonpost.com/wp-dyn/content/article/2010/11/29/AR2010112903468.html> accessed 15 November 2016.

[30] Ibid.

[31] Kessler (n 14).

Therefore, while the states involved have not officially confirmed it, Stuxnet is believed to have been created by state actors to disrupt the operation of a uranium enrichment facility in another state. Unlike previously known or suspected incidents involving malicious cyber activities by states, however, Stuxnet is the first known incident of state actors using cyber means to cause damage to physical property in another state. Accordingly, a key issue raised by the incident is whether a cyberattack of this kind can constitute a violation of international law prohibiting states from using 'force' in their international relations.

3 THE ARTICLE 2(4) PROHIBITION ON THE USE OF FORCE

This part first provides an overview of the orthodox approach to the prohibition of the use of force in the non-cyber context contained in Article 2(4) of the Charter of the United Nations (UN Charter). The focus is on the notion of 'force' in relation to cyberattacks below the armed attack threshold. It then considers existing scholarship on cyberattacks and the law on the use of force, and looks at how the law has been applied to the Stuxnet incident. It is argued that the orthodox approach to the use of force reflects an anthropocentric and materialist view of violence. The law has a narrow focus on violence involving damage or destruction of physical property, or injury or death of human beings. As such, it lacks the adequate ability to recognise harm to non-material entities and appreciate the harm that can be caused to states that increasingly rely on ICTs for their proper functioning.

3.1 The orthodox approach to Article 2(4)

The Article 2(4) prohibition of the use of force, particularly the meaning of the notion of 'force' that it embodies, represents the central doctrine through which interstate violence is understood.[32] As a key rule of international law within the UN Charter era, Article 2(4) seeks to limit interstate violence by prohibiting states from using force in their international relations.[33] However, the ambiguous notion of 'force' is not defined in the UN Charter and there has been debate about its meaning.[34] While acts of military aggression by states are clearly considered to constitute uses of force,[35] controversy has surrounded what other types of force fall within its ambit. For example, when Article 2(4) was drafted the Brazilian delegation suggested that it should also include economic coercion; however, this view was rejected at the time.[36] Thus the prevailing view is that force only refers to *armed* force, whereas other forms of economic or political coercion can only constitute a breach of the non-intervention principle.[37] This view aligns with the intention of the drafters, who deemed at the time that the use of armed force in particular was 'simply too destructive to be considered an acceptable means of pursuing changes or advancing other policy'.[38] It is also supported by UN General Assembly resolutions that refer to the prohibition of the use of force in the context of military force, whereas economic and political coercion are referred to in the context of the duty not to intervene in the internal matters of a state.[39]

---

[32] Violence in this context essentially refers to direct intentional acts of harm towards a state and, as will be shown, only certain types of harm are capable of being recognised within the conception of violence that underpins the notion of force.

[33] The ICJ has described the provision as 'the very cornerstone of the human effort to promote peace in a world torn by strife.' *Case Concerning Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v United States of America)* (Merits) (Separate Opinion of President Nagendra Singh) [1986] ICJ Rep 14, 153.

[34] Michael 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; Albrecht Randelzhofer, 'Article 2(4)' in Bruno Simma and others (eds), *The Charter of the United Nations: A Commentary Volume 1* (OUP, Oxford 2002) 117.

[35] See UNGA Res 3314 (XXIX) (14 December 1974) UN Doc A/RES/29/3314.

[36] See Randelzhofer (n 34) 118; Schmitt (n 34) 905.

[37] *Case Concerning Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v United States of America)* (Merits) [1987] ICJ Rep 14, 108.

[38] Anthony Arend and Robert Beck, *International Law and the Use of Force: Beyond the UN Charter Paradigm* (Routledge, London 1993) 34.

[39] UNGA Res 2625 (XXV) (24 October 1970) UN Doc A/RES/25/2625; UNGA Res 42/22 (18 November 1987) UN Doc A/42/766). See also Schmitt (n 34) 907.

Accordingly, it is generally accepted that the notion of 'force' within Article 2(4) refers to armed force.[40]

Since its inception, however, questions have been raised as to whether the use of non-kinetic weapons, such as chemical and biological weapons, constitute uses of 'armed' force. Ian Brownlie famously maintained that such weapons should constitute uses of force due to the common reference to them as 'weapons' and, more importantly, due to their employment 'for the destruction of life and property'.[41] He placed importance not only on the weapon-like nature of the instruments used, but also on their destructive effects, in determining whether their use would breach Article 2(4). Similarly, the International Court of Justice (ICJ) has noted that Article 2(4) does not refer to specific weapons, meaning the provision applies 'to any use of force, regardless of the weapons employed'.[42] As such, even with the development of chemical, biological and nuclear weapons technologies, any use of force contemplated to be prohibited by Article 2(4) clearly requires the use of weapon-like instruments capable of causing injury or death to humans, or damage or destruction of physical property.

In addition to these forms of military force, some have also discussed whether physical non-military force can constitute 'force' for the purposes of Article 2(4). Brownlie, for example, argues that, where one state controlling the upper reaches of a river releases water downstream, the 'deliberate employment of natural forces by a state in such circumstances can probably be regarded as a use of force'.[43] Others have taken a similar view.[44] As such, physical non-military force, like the deliberate release of large quantities of water or spread of fire, can also constitute 'force' where it injures human beings or damages property.

As is evident in the accepted view of what constitutes 'force' under Article 2(4), the law embodies a limited conception of violence. It is an anthropocentric and materialist conception, as any use of force that injures or kills human beings, or damages or destroys physical objects is seen to constitute a form of violence capable of crossing the use of force threshold. This is particularly evident in the debate about whether the use of non-kinetic weapons or destructively used non-military force can constitute a use of force, where the answer is clearest when human beings are injured or physical objects are damaged. As the next section will demonstrate, however, advances in technology in the context of cyberattacks problematise this particularly because the harm or damage caused by such attacks is less often solely to human beings or material objects.

3.2 The orthodox approach to Article 2(4) and cyberattacks

The question of whether cyberattacks can constitute a use of force has been examined by numerous legal scholars since the 1990s.[45] The issue has become particularly prominent following a number of incidents such as the 2007 cyberattacks against Estonia and the cyberattacks against Georgia in 2008.[46] In determining whether a cyberattack constitutes a use of force, three different approaches are evident in legal scholarship. 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, it may amount to a use of armed force.[47] The 'target approach' in turn focuses on the

[40] Stephen Neff, 'Economic Warfare in Contemporary International Law: Three Schools of Thought, Evaluated According to an Historical Method' (1989) 26 Stanford Journal of International Law 67, 83; Schmitt (n 34) 908; Yoram Dinstein, *War, Aggression and Self-Defence* (3rd edn, CUP, Cambridge 2001) 81; Randelzhofer (n 34) 117; Antonio Cassese, *International Law* (OUP, Oxford 2005) 56.

[41] Ian Brownlie, *International Law and the Use of Force by States* (Clarendon Press, Oxford 1963) 362.

[42] *Legality of the Threat or Use of Nuclear Weapons* (Advisory Opinion) [1996] ICJ Rep 226, 244.

[43] Brownlie (n 41) 376. See also Randelzhofer (n 34) 118.

[44] See Randelzhofer (n 34) 119; Daniel 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, 83.

[45] See, for example, Walter Sharp, *CyberSpace and the Use of Force* (Aegis Research Corporation, Falls Church 1999); Schmitt (n 34).

[46] For an overview of the Estonia and Georgia incidents and surrounding legal issues, see Eneken Tikk, Kadri Kaska and Liis Vihul, *International Cyber Incidents: Legal Considerations* (NATO Cooperative Cyber Defence Centre of Excellence, Tallinn 2010).

[47] See Duncan Hollis, 'Why States Need an International Law for Information Operations' (2007) 11 Lewis & Clark Law Review 1023, 1041; David Graham, 'Cyber Threats and the Law of War' (2010) 4 Journal of National Security Law and Policy 87, 91; Oona Hathaway and others, 'The Law of Cyber-Attack' (2012) 100 California Law Review

target of the cyberattack—where this is important infrastructure, for instance, it should be considered a use of force.[48] Finally, the 'effects approach' is concerned with the effects of cyberattacks and whether they are comparable to those of conventional military attacks.[49] Few adopt a single approach by itself, and these are more so used to distinguish between various considerations in assessing whether a cyberattack amounts to a use of force. Marco Roscini for instance combines the 'instrument approach' and 'effects approach', suggesting that whether a cyberattack amounts to a use of force or not must be determined by the weapons used (instruments); however, 'weapons' are defined by the harmful effects of the instrument in question.[50] Accordingly, for Roscini it is the 'instrument used that defines armed force, but the instrument is identified by its (violent) consequences'.[51] Similarly, William Boothby adopts the position that a cyber weapon is defined by its violent consequences—where a means of cyberattack is 'designed, intended or used, in order to have violent consequences, that is, to cause death or injury to persons or damage or destruction of objects.'[52]

Under the 'effects approach', which has attracted the most support by authors, a cyberattack is assessed based on its effects and whether they are akin to a use of armed force. As such, cyberattacks 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. Relying on Brownlie's effects-based approach focusing particularly on whether there was any 'destruction of life or property',[53] Jason Barkham for instance argues that cyberattacks that cause instantaneous destruction akin to that caused by conventional weapons are 'relatively easy' to regard as constituting uses of force.[54] Michael Schmitt also notes that the narrow category of cyberattacks 'specifically intended to directly cause physical damage to tangible property or injury or death to human beings' are 'easily dealt with.'[55] For Heather Harrison Dinniss it 'appears to be clear' that a cyberattack will constitute a use of force where it 'results in a physical consequence, namely destruction of physical property, injury or loss of lives'.[56] Yoram Dinstein also maintains that the crux of whether a cyberattack amounts to a use of force is not the means used but its 'violent consequences'.[57] A number of other authors take a similar view.[58]

In addition to legal scholarship on the issue of when a cyberattack constitutes force, the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Tallinn Manual) provides an important soft-law instrument in this area.[59] On the issue of when a cyberattack crosses the use of force threshold, the Tallinn Manual provides in Rule 69 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'.[60]

817, 845–847; Marco Roscini, *Cyber Operations and the Use of Force in International Law* (OUP, Oxford 2014) 46–47.

[48] Hollis (n 47) 1041; Graham (n 47) 91; Hathaway and others (n 47) 846–847; Roscini (n 47) 47.

[49] Ibid.

[50] Roscini (n 47) 49–50.

[51] Ibid 50.

[52] William H. Boothby, 'Methods and Means of Cyber Warfare' (2013) 89 International Law Studies Series US Naval War College 387, 389.

[53] Jason Barkham, 'Information Warfare and International Law on the Use of Force' (2001) 34 New York University Journal of International Law and Politics 57, 72 citing Brownlie (n 41) 362–363.

[54] Ibid 80.

[55] Schmitt (n 34) 913.

[56] Heather Harrison Dinniss, *Cyber Warfare and the Laws of War* (CUP, Cambridge 2012) 74.

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

[58] See, for example, 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; Herbert S. Lin, 'Offensive Cyber Operations and the Use of Force' (2010) 4 Journal of National Security Law and Policy 63, 73; Katharina Ziolkowski, 'Computer Network Operations and the Law of Armed Conflict' (2010) 49 Military Law and the Law of War Review 47, 70; Roscini (n 47) 53.

[59] Michael N. Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2nd edn, CUP, Cambridge 2017). See also Michael N. Schmitt (ed), *Tallinn Manual on the International Law Applicable to Cyber Warfare* (CUP, Cambridge 2013).

[60] Schmitt, *Tallinn Manual 2.0* (n 59) 330.

In essence, Rule 69 answers the threshold question that a cyberattack will constitute a use of force where it is comparable in scale and effects to a use of force as traditionally understood. In the commentary to the rules, the authors note that generally '[a]cts that injure or kill persons or physically damage or destroy objects are uses of force'[61] and that where cyberattacks involve similar consequences they will qualify as uses of force.[62] The authors also provide a number of factors that can be considered in making the assessment of when a cyberattack constitutes a use of force.[63] Here too they stress that the severity of an attack is the 'most significant' criterion to be considered.[64]

The non-material effects of cyberattacks—and also cyberattacks without any material effects—are more problematic. Non-material effects, such as where the operation of computer systems or networks is disrupted without destruction of hardware, or only the integrity of information is undermined, are difficult to characterise as uses of force.[65] Again this is evident in legal scholarship on cyberattacks and Article 2(4). 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'.[66] Barkham also recognises that cyberattacks which only undermine the integrity of data, as opposed to actually destroying it, would not be considered uses of force as there is no weapon involved nor property destroyed.[67] Roscini similarly highlights how it is 'very difficult to answer' whether the destruction of data can be equated to the destruction of physical property that would fall under Article 2(4).[68] Boothby in turn 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'.[69] 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 the functioning of the computer systems or networks to the degree that repairs are needed for them to operate again.[70]

Accordingly, the orthodox approach to cyberattacks and the use of force also demonstrates the law's anthropocentric and materialist conception of violence. The prevailing view is that cyberattacks resulting in injury or death of human beings, or damage or destruction of physical property constitute the 'easy cases' for the use of force analysis. In other words, cyberattacks causing direct harm to human beings or material damage to physical objects fit neatly within the law's view of violence. However, the law has difficulty recognising the non-material effects of cyberattacks, such as damage or disruption to virtual entities and processes that result in the disruption of the operation of computer systems and networks, but not their destruction. Essentially, the type of harm caused by such attacks is not something that Article 2(4) is capable of recognising within the conception of violence underpinning it.[71] This is demonstrated by the tendency to consider the non-material effects of cyberattacks as falling below the use of force threshold or as otherwise problematic for the use of force analysis. As the next section will

---

[61] Ibid 333.
[62] Ibid.
[63] See ibid 334–336. These criteria are based on criteria that Michael Schmitt first suggested in the late 1990s. Schmitt (n 34) 914–915.
[64] Schmitt, *Tallinn Manual 2.0* (n 59) 334. They also note that the severity of an attack is influenced by its scope, duration, and intensity.
[65] Authors tend to argue that cyberattacks without material effects, provided the element of coercion is present, constitute breaches of the non-intervention principle instead. See, for example, Joyner and Lotrionte (n 58) 849; Marco Benatar, 'The Use of Cyber Force: Need for Legal Justification?' (2009) 1 Goettingen Journal of International Law 375, 395; Dinniss (n 56) 74; Roscini (n 47) 115.
[66] Dinniss (n 56) 68.
[67] Barkham (n 53) 89.
[68] Roscini (n 47) 55.
[69] Boothby (n 52) 389.
[70] Ibid 389–390.
[71] Similarly, under conventional understandings of what constitutes 'violence', cyberattacks are generally not regarded as such. For example, according to Thomas Rid, because human beings cannot be directly harmed through cyber means in the same way as they can through energy (such as heat or a laser), or chemical or biological agents, 'most cyberattacks are not violent and cannot sensibly be understood as a form of violent action'. Thomas Rid, *Cyber War Will Not Take Place* (OUP, Oxford 2013) 12–13.

demonstrate, while Stuxnet is widely considered to have constituted a use of force, the primary factor for making this determination is its effects in the physical world.

3.3 The orthodox approach to Article 2(4) and Stuxnet

Stuxnet is widely considered in relation to the question of when a cyberattack crosses the use of force threshold. The majority of authors, accepting that Stuxnet was the cause of the destruction of approximately 1000 centrifuges, maintain that it constituted a use of force particularly as it caused material damage to physical objects. For example, Gary Brown points to the fact that Stuxnet was '[i]ntentionally designed malware directed against a nation-state [and] resulted in the physical destruction of state-owned equipment. The centrifuges were destroyed as effectively as if someone had taken a hammer to them'.[72] He therefore maintains that the incident violated the general prohibition on the use of force.[73] Also, according to a number of authors including Boothby and Schmitt, Stuxnet qualifies as a use of force '[b]ecause the facilities suffered physical damage'.[74] Therefore, for these authors, since Stuxnet caused material damage to physical objects, it clearly constituted a use of force.

A number of authors also consider Stuxnet in relation to the Tallinn Manual criteria.[75] In this context, most highlight the physical damage caused by Stuxnet in relation to the 'severity' criterion. For example, David Weissbrodt argues that 'Stuxnet, at minimum, is considered to be a use of force'.[76] In relation to the severity criterion he notes that 'the Stuxnet attack was severe because it caused physical harm to property. Stuxnet caused the centrifuges to speed up and slow down their rotation causing them to break'.[77] Various others similarly adopt this position,[78] and the authors of the Tallinn Manual also take the view that Stuxnet amounted to a use of force.[79]

Given that Iran has not confirmed the destruction of centrifuges, some authors question whether Stuxnet was responsible for their destruction. Katharina Ziolkowski, for example, maintains that whether Stuxnet constituted a use of force within the meaning of Article 2(4) depends on whether it 'caused a non-trivial destruction of property'.[80] She argues that if indeed Stuxnet 'did not cause any damage of physical nature, it appears not to reach the threshold of illegality pursuant to public international law and thus to be a "legal masterpiece".'[81] Similarly, Russell Buchan maintains that if Stuxnet simply 'prevented the centrifuges from rotating at the correct speed' meaning that uranium could not be enriched without the actual destruction of centrifuges, then Stuxnet 'cannot be regarded as an unlawful use of force because no damage to physical property was caused'.[82] However, he argues that if the reports that Stuxnet did cause the physical destruction of centrifuges are correct, then 'this would constitute the requisite physical

---

[72] Gary Brown, 'Why Iran Didn't Admit Stuxnet Was an Attack' (2011) 63 Joint Force Quarterly 70, 71 (citations omitted).
[73] Ibid.
[74] William Boothby and others, 'When is a Cyberattack a Use of Force or an Armed Attack?' (2012) 45(8) Computer 82, 83. For similar positions, see also David P. Fidler, 'Was Stuxnet an Act of War? Decoding a Cyberattack' (2011) 9(4) IEEE Security & Privacy 56, 57; Dinniss (n 56) 81–82; Andrew Moore, 'Stuxnet and Article 2(4)'s Prohibition Against the Use of Force: Customary Law and Potential Models' (2015) 64 Naval Law Review 1, 1.
[75] Some of these authors consider the Tallinn Manual criteria specifically, whereas others consider Schmitt's criteria (which formed the basis for the Tallinn Manual criteria).
[76] David Weissbrodt, 'Cyber-Conflict, Cyber-Crime, and Cyber-Espionage' (2013) 22 Minnesota Journal of International Law 347, 376.
[77] Ibid.
[78] See Andrew C. Foltz, 'Stuxnet, Schmitt Analysis, and the Cyber "Use-of-Force" Debate' (2012) 67 Joint Force Quarterly 40, 44; Charles C. Poché, 'This Means War! (Maybe?) – Clarifying Casus Belli in Cyberspace' (2013) 15 Oregon Review of International Law 413, 433–434; Priyanka R. Dev, '"Use of Force" and "Armed Attack" Thresholds in Cyber Conflict: The Looming Definitional Gaps and the Growing Need for Formal UN Response' (2014) 50 Texas International Law Journal 379, 395.
[79] See Schmitt, *Tallinn Manual 2.0* (n 59) 342.
[80] Katharina Ziolkowski, 'Stuxnet – Legal Considerations' (2012) 25 Humanitäres Völkerrecht – Informationsschriften / Journal of International Law of Peace and Armed Conflict 139, 142.
[81] Ibid 147.
[82] Russell Buchan, 'Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?' (2012) 17 Journal of Conflict & Security Law 211, 220.

damage in order for a violation of Article 2(4) to be established'.[83] As such, while these authors do not take a clear position on whether Stuxnet in fact constituted a use of force, they nonetheless highlight the importance of physical damage in making this determination.

As these analyses of Stuxnet in light of Article 2(4) highlight, the law requires known physical damage for a cyberattack to constitute a use of force. Stuxnet is generally considered to have crossed this threshold. This is almost exclusively because it caused damage to approximately 1000 centrifuges; or, alternatively, the primary obstacle for making this determination is the lack of sufficient certainty that it in fact had this effect. The orthodox approach to Article 2(4) and Stuxnet therefore demonstrates the law's anthropocentric and materialist conception of violence. Had Stuxnet injured human beings it would undoubtedly have been considered to have crossed the use of force threshold. While this was not the case, because it is believed to have caused damage to physical objects, its effects align with what the law is capable of recognising as a form of violence.

However, this is a one-dimensional account of violence that does not adequately capture the non-material harm that Stuxnet caused. Despite the range of ways in which Stuxnet undermined the integrity of thousands of computers within Iran and disrupted the proper operation of the computers within the Natanz enrichment facility, the primary focus of these analyses is the physical damage to centrifuges. This limited conception of violence is also evident in the view that, had Stuxnet alternatively only disrupted the operation of the uranium enrichment process and not actually physically damaged centrifuges, it is unlikely to have been considered a use of force.[84] In this scenario there would have been little real difference in terms of Stuxnet's overall effect in undermining Iran's ability to properly enrich uranium with those centrifuges. However, the law would not have been able to recognise the incident as a form of violence under Article 2(4) due to the lack of physical damage. As the next part will demonstrate, an informational approach offers a deeper account of the violence that Stuxnet effected. It does so by accounting for the harm that Stuxnet caused not simply by damaging physical objects, but also by disrupting or undermining of the proper operation of countless virtual entities and processes associated with the functioning of the Natanz enrichment facility.

4 AN INFORMATIONAL APPROACH

This part argues that an informational approach offers a means to rethink the limited conception of violence evident in the orthodox approach to cyberattacks and Article 2(4). By recognising a broader ontological spectrum of entities capable of being harmed, the law's narrow focus on human beings and physical objects can be expanded to account for the non-material effects of cyberattacks. By adopting an alternative ontology, the harm caused by cyberattacks—whether physical or not—can be thought about more universally in terms of their impact on all information entities and the infosphere as a whole. As such, this approach provides a way to update the ontology underpinning the law's conception of violence to account for the new ways in which states that increasingly rely on ICTs for their proper functioning can be harmed through cyberattacks. As one of Article 2(4)'s key aims is to limit interstate violence by creating a general prohibition on the use of force, a reconceptualisation of the notion of violence that underpins it can enable recognition of a broader range of cyberattacks within the prohibition. This part first provides an overview of Luciano Floridi's information ethics. Drawing on this conceptual framework, it then considers the harm caused by cyberattacks and develops an informational approach to the Stuxnet incident to demonstrate how the harm caused by Stuxnet can be rethought.

4.1 Information ethics – an overview

Floridi's 'information ethics'[85] is best described as a form of environmental ethics that extends its ethical concern beyond the physical environment to include digital environments and entities.

[83] Ibid 220–221.
[84] See Foltz (n 78) 45; Buchan (n 82) 220.
[85] 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* (OUP, Oxford 2013). On information ethics and cyber

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.[86] 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.[87]

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'.[88] 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.[89] As such, by adopting a perspective from which all entities can be viewed in terms of their information structures, all entities can be seen as information entities.[90] 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.[91] 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.[92]

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'.[93] 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, for example, thermodynamics. In his use of the term, it essentially refers to any degradation of being, such as the destruction or corruption of information entities.[94]

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.[95] Information ethics therefore provides an environmental approach to thinking about what is good

---

warfare, see Mariarosaria Taddeo, 'Information Warfare: A Philosophical Perspective' (2012) 25 Philosophy & Technology 105; 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; Mariarosaria Taddeo, 'Just Information Warfare' (2016) 35 Topoi 213. See also Massimo Durante, 'Re-designing the Role of Law in the Information Society: Mediating between the Real and the Virtual' (2010) 2(3) 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.

[86] Luciano Floridi, *Information: A Very Short Introduction* (OUP, Oxford 2010) 111.

[87] Ibid 112.

[88] Floridi, 'Information Ethics' (n 85) 44. See also Floridi, *The Ethics of Information* (n 85) 6; Luciano Floridi, *The Fourth Revolution* (OUP, Oxford 2014) 41.

[89] Luciano Floridi, 'Information Ethics, Its Nature and Scope' (2006) 36(3) Computers and Society 21, 33.

[90] Ibid.

[91] Floridi, *Information* (n 86) 113.

[92] Floridi, 'Information Ethics' (n 85) 44.

[93] Floridi, *Information* (n 86) 113.

[94] Floridi, *The Ethics of Information* (n 85) 67.

[95] 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 well-being.

for the infosphere and offers an approach that advocates respect for both the material and non-material world.[96]

4.2 Informational violence

A number of authors have considered Floridi's information ethics in the context of cyber warfare.[97] For example, both Mariarosaria Taddeo and Ugo Pagallo have considered the traditional just war principles in the context of the four moral laws of information ethics to explore the morality of cyber warfare.[98] The focus here, however, is particularly on the harm caused by cyberattacks and how the law reflects a limited view of violence that is only capable of recognising harm to physical entities within Article 2(4).

Other authors have also sought to reconsider the harm in cyberattacks. For example, Randall Dipert suggests an ontological rethinking of the harm caused by cyberattacks. He maintains that this should involve a shift in 'focus away from strictly injury to human beings and physical objects toward a notion of the (mal-)*functioning* of information systems, and the other systems (economic, communication, industrial production) that depend on them'.[99] He proposes the notion of cyber harm as harm inflicted through cyberspace in which 'the functioning of a system (a person, a machine, software or an economy) is in some way impaired or degraded'.[100] Massimo Durante also considers the notion of violence specifically from an information ethics perspective, distinguishing between informational and physical violence. He argues that physical violence arises 'when a disruptive activity damages, deteriorates, deletes or suppresses an informational object'[101]—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.[102] He argues that moral violence in informational terms occurs when an entity is deprived of its capacity to flourish and become a specific source of information and hence become an agent.[103] It is a form of 'radical regardlessness' towards an entity.[104]

The informational reconceptualisation of violence offered here is similar to both of these accounts. Like Dipert's cyber harm, the concern is with harm to the functioning of an entity, that is, its impairment or degradation which is captured by the notion of entropy. Also like Durante's account of physical and informational violence, a distinction is made between the two in order to highlight the material and non-material dimensions of cyberattacks. The primary focus here, however, is on how cyberattacks undermine the integrity of states 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 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 damage, destruction, degradation, corruption or pollution of an entity, impacting on its very being and right to exist.[105] While Floridi maintains that the notion of harm is problematic, as it implies that the

---

[96] Luciano Floridi, 'Information Ethics: An Environmental Approach to the Digital Divide' (2002) 9(1) Philosophy in the Contemporary World 39, 42.
[97] See Taddeo, 'Information Warfare' (n 85); Taddeo, 'Just Information Warfare' (n 85); Pagallo, 'Cyber Force' (n 85); Durante, 'Violence, Just Cyber War' (n 85).
[98] These authors mainly adopt the four principles of information ethics and merge them with just war principles to consider the legitimacy of the circumstances in which cyberattacks, for instance, can be used. See Taddeo, 'Just Information Warfare' (n 85) 221–222; Pagallo, 'Cyber Force' (n 85).
[99] Randall R. Dipert, 'The Ethics of Cyberwarfare' (2010) 9 Journal of Military Ethics 384, 386.
[100] Ibid 397.
[101] Durante, 'Violence, Just Cyber War' (n 85) 383.
[102] Ibid 382–83.
[103] Ibid 383.
[104] Ibid.
[105] As Floridi writes, it is an 'impoverishment of *Being*'. Floridi, *The Ethics of Information* (n 85) 67.

object of harm is a 'sentient being with a nervous system',[106] 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.[107] 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.[108] 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.[109]

Viewing the harm inherent in any act of violence in terms of entropy, however, means that on one level with everything viewed in informational terms, all forms of violence can be seen as 'informational violence'. For example, intentional acts of physical harm to an entity resulting in damage, destruction, injury or death—that is, physical violence—can also be seen as causing entropy by destroying or degrading the informational structures the entity is made of. However, in order to distinguish between physical violence and forms of violence that do not result in damage or injury to, or destruction or death of, an entity, the notion of informational violence will be used in a narrower sense. This allows a distinction between the material effects of cyberattacks that can be likened to a form of physical violence, and the non-material effects of cyberattacks. Accordingly, the notion of informational violence is used here to refer to intentional acts of non-material harm to an entity. This is to distinguish informational violence from physical violence which involves material harm to an entity. Therefore, cyberattacks can be seen as forms of informational and/or physical violence depending on whether they cause non-material and/or material harm, and in both cases their impact can be considered in terms of the increases in entropy they produce and their impact on the infosphere.

The remainder of this part draws on the publicly available technical details about Stuxnet to offer an informational approach to the incident.[110] It demonstrates that this approach provides a way in which to consider a cyberattack's effects on a range of material and non-material entities and processes. Through this approach, Stuxnet can be seen as inflicting both informational and physical forms of violence causing increases in entropy within the Natanz facility.

4.3 An informational approach to Stuxnet

Stuxnet was a technically sophisticated piece of malicious software and demonstrated that its designers had extensive knowledge of the Natanz enrichment facility. It was specifically designed to undermine the operation of Iran's nuclear programme by causing increased entropy within the

---

[106] 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.

[107] 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* (OUP, Oxford 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. Feinberg 33.

[108] 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 33.

[109] 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, *The Ethics of Information* (n 85) 70–72.

[110] In late September 2010 Symantec released a dossier containing its technical analysis of Stuxnet. The final version of this dossier was released in February 2011 (version 1.4). Falliere, Murchu, and Chien (n 10). A follow-up report entitled 'Stuxnet 0.5: The Missing Link' was released in 2013. Geoff McDonald and others, 'Stuxnet 0.5: The Missing Link' (Symantec 2013) <www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/stuxnet_0_5_the_missing_link.pdf> accessed 15 November 2016.

Natanz facility. However, the degrees of entropy produced by various parts of Stuxnet varied, ranging from undermining the integrity of computers and exploiting the communication protocols between computers, to delivering a payload causing physical damage to approximately 1000 centrifuges.

4.3.1 Propagation methods

The original infection method and propagation methods used by Stuxnet allowing the introduction and spread of Stuxnet into and throughout Iran resulted in various degrees of increases in entropy. While it remains unknown exactly how and when Stuxnet 0.5 (the earliest known version of Stuxnet) was introduced into Natanz, from the information obtained from Stuxnet's log file, the June 2009, March 2010, and April 2010 variants first infected the computers of five separate companies.[111] Through these computers Stuxnet then spread into the Natanz facility. The initial infection of the first computers within these companies can only be considered a very minor increase in entropy. However, over time approximately 12,000 computers within these corporate entities were infected,[112] leading to a larger increase in entropy given the total amount of infected computer systems. Stuxnet ultimately spread and infected over 100,000 computers around the world, which in turn can be regarded as a more significant increase in entropy. Over 60,000 of these were located within Iran.[113] While these computers continued to operate normally, their integrity was compromised. Stuxnet would for example check which anti-virus software was installed on a computer and choose the most appropriate injection process into that computer, and if necessary also exploit a zero-day vulnerability to inject itself into an active process run by the computer.[114] Without the authorisation of the legitimate users, Stuxnet also granted itself administrator rights through the exploitation of zero-day vulnerabilities.[115] It was therefore capable of bypassing the security mechanisms of each computer system which were designed to protect these entities from threats capable of causing increases in entropy.

Further, given that Stuxnet had administrator rights on each computer, it was capable of taking any action it wanted.[116] While it only delivered its payload to very specific computer configurations and only sent basic information about the other computers it infected to the command and control servers, it is understood to have had the ability to download additional features from these servers.[117] Though it did not disrupt the operation of these computers, it had undermined their integrity and was able to communicate with other computers infected by Stuxnet and the command and control servers, update itself, and even potentially obtain additional features. As such, in addition to the entropy caused in undermining the integrity of these computers in the above ways, Stuxnet also had a further potential to cause more increases in entropy in the over 100,000 entities it had infected.

By infecting these computers Stuxnet was able to reach the programmable logic controllers (PLCs) used to operate the centrifuge machines.[118] The computers used to program PLCs (and the PLCs themselves) were specifically configured so as to protect them from entropy and keep them secure from potential threats that could come through the internet.[119] Through an air-gap preventing the flows of digital information into these computers, Iran sought to protect the integrity of these computers and the processes they were used to operate within the Natanz facility. As such, the Natanz facility's interactions with other entities, even within Iran, were

[111] Falliere, Murchu, and Chien (n 10) 8–11.
[112] Zetter (n 15) 97–98.
[113] Falliere, Murchu, and Chien (n 10) 6.
[114] Ibid 14. A zero-day vulnerability is an 'unpatched software hole' that is unknown to the vendor of the software. Kim Zetter, 'Hacker Lexicon: What Is a Zero Day?' *Wired* (11 November 2014) <www.wired.com/2014/11/what-is-a-zero-day> accessed 24 January 2018.
[115] Falliere, Murchu, and Chien (n 10) 16–17.
[116] Ibid.
[117] Ibid 22.
[118] A programmable logic controller (PLC) is a special computer often used to program industrial equipment. William Bolton, *Programmable Logic Controllers* (5th edn, Newnes, Oxford 2009) 3.
[119] Falliere, Murchu, and Chien (n 10) 3; Kim Zetter, 'Hacker Lexicon: What Is an Air Gap?' *Wired* (8 December 2014) <www.wired.com/2014/12/hacker-lexicon-air-gap> accessed 15 November 2016.

limited to those with physical access to it. Consequently, the attackers exploited other information flows into the Natanz facility in order infect it with Stuxnet. These included, for example, programmers and engineers with physical access to the Natanz facility.[120] Stuxnet was able to copy itself onto USB drives using a driver file which was signed with a stolen digital certificate which meant that it would be trusted by the system as a safe file.[121] It also exploited a zero-day vulnerability in .LNK files to execute automatically when the USB drive was inserted into a new computer.[122] As the main propagation method used, by spreading to and from USB drives, Stuxnet was able to spread across the computers of humans working for corporate entities involved with Iran's nuclear program and consequently obtain access to the secure Natanz facility.[123] Therefore, while the Natanz facility was disconnected from the internet, Stuxnet exploited other information flows into it and produced entropy by undermining the integrity of the Natanz facility.

In addition to the entropy caused by Stuxnet in the process of undermining the integrity of the Natanz facility, the various other propagation methods used to further spread and reach the PLCs also caused increases in entropy. In addition to USB drives, the propagation methods also made use of peer-to-peer (P2P) connectivity and Local Area Networks (LANs),[124] and involved the exploitation of information exchanges between entities. For example, by exploiting the print-spooler vulnerability of computers connected to a shared printer through a LAN, Stuxnet enabled unauthorised information exchanges between these computers and used these exchanges to spread.[125] Also, by infecting the project files used by the Siemens Step 7 software that is used to program PLCs, Stuxnet was able to spread to computers using this software and hence also to those computers used to configure PLCs.[126] Therefore, Stuxnet caused increases in entropy by undermining and degrading the integrity of the normal information exchange processes between computers sharing a printer on a LAN, and between computers using Step 7 software to access project files. Finally, by exploiting P2P connectivity within a LAN, Stuxnet enabled information exchanges to and from computers that had been configured to be secure and disconnected from the internet.[127] This way, Stuxnet could communicate with computers not connected to the internet and relay information about these computers to the command and control servers. In addition to causing increases in entropy by undermining the integrity of these computers, Stuxnet also did so by undermining the non-networked configuration of these computers. Through these propagation methods collectively, Stuxnet was able to undermine the integrity of these computers and their interactions, and it ultimately undermined the integrity of the PLCs it reached using these methods. Doing so caused increases in entropy within the infected computer systems and within the Natanz facility as a whole.

4.3.2 Man-in-the-middle

Besides the entropy produced by Stuxnet's propagation methods, the man-in-the-middle attack also produced increases in entropy.[128] Stuxnet replaced the legitimate library file that is used by the Step 7 software to communicate with PLCs with its own version.[129] This allowed Stuxnet to monitor the data sent to and from the PLC, to send its own data or replace existing data being sent to and from the PLC, and hide the fact that the PLC was infected.[130] As a result, Stuxnet was capable of intercepting and manipulating the data that was communicated between the computer operating Step 7 software and the PLC used to configure the operation of the centrifuge cascades.

---

[120] Sanger (n 23).
[121] Falliere, Murchu, and Chien (n 10) 24.
[122] Ibid 29.
[123] Liam O Murchu, 'Countdown to Zero Day – Did Stuxnet escape from Natanz?' (Symantec Official Blog 2014) <www.symantec.com/connect/blogs/countdown-zero-day-did-stuxnet-escape-natanz> accessed 13 February 2018.
[124] Falliere, Murchu, and Chien (n 10) 25–26.
[125] Ibid 27–28; Zetter (n 15) 90.
[126] Falliere, Murchu, and Chien (n 10) 25, 33.
[127] Ibid 26.
[128] This term is used to describe 'an unseen relay that intercepts, understands, alters, and retransmits a message for the purpose of deception'. Richard E. Blahut, *Cryptography and Secure Communication* (CUP, Cambridge 2014) 511.
[129] Falliere, Murchu, and Chien (n 10) 37–38.
[130] Ibid 36.

Using the data that Stuxnet had obtained during its monitoring phase, the man-in-the-middle attack allowed it to feed data showing the normal operation of the frequency controllers to the operators of the Natanz facility and prevented them from receiving 'the anomalous operating frequency data'[131] that would otherwise have been sent while it delivered its payload. This undermined the integrity of the information that was being relayed from the Step 7 software to the PLC used to operate centrifuge machines, and the information relayed to and relied upon by the human operators of the Natanz facility. Also, by replacing the library file with a malicious version, Stuxnet undermined the integrity of relationship between the Step 7 software and the PLC it was used to configure. By doing so and undermining the integrity of this information exchange process, Stuxnet caused further increases in entropy. Additionally, by infecting a particular data block used by the PLC as a safety mechanism for when it is faced with catastrophic events, Stuxnet prevented the operation of digital alarm systems that would otherwise have been triggered.[132] Stuxnet prevented the PLC from executing this data block during its sabotage routine, and this is understood to have prevented the system's automatic shutdown that would normally occur during catastrophic events.[133] Stuxnet therefore disabled a protective function that would otherwise have indicated that a component of the Natanz facility was threatened by an entity capable of causing increased entropy.

4.3.3 Payload

In addition to the various degrees of entropy caused by Stuxnet's propagation methods and its man-in-the-middle attack, the most significant amount of entropy was caused by its payload. Among the necessary conditions required by Stuxnet before it delivered its payload was that it had found a S7-315 model PLC used to operate a frequency converter drive manufactured by either Fararo Paya or Vacon[134] which was operating at between 807 Hz and 1210 Hz.[135] Then, during the third and fourth states of its 27-day attack cycle, Stuxnet sent bursts of data containing instructions determining the operation of the frequency converter drives used to control the rotation speed of the centrifuges.[136] In the first cycle, Stuxnet adjusted the frequency of the frequency converter drive to 1410 Hz for 15 minutes and then back to 1064 Hz.[137] This resulted in an increase in the rotation speed of the centrifuge that is believed to be sufficient to both disrupt the enrichment process and destroy the centrifuge.[138] Approximately 27 days later in the third and fourth states of the second cycle, Stuxnet sent another burst of data adjusting the frequency to 2 Hz for 50 minutes then back to 1064 Hz, meaning the centrifuge rotors were slowed down.[139] This is believed to have degraded the uranium enrichment process meaning a lower amount of uranium was enriched.[140] As such, Stuxnet altered the information sent from the PLC to the frequency converter drives, and as the normal operation frequency of these devices is between 807 Hz and 1210 Hz,[141] it corrupted the normal properties of these entities when used for uranium enrichment. The combined result of the two cycles demonstrated that Stuxnet was intended to induce 'excessive vibrations or distortions' capable of physically damaging the centrifuge.[142] In addition to the entropy caused by the corruption of the frequency converter drives and the consequent disruption of the normal operation of the centrifuges, Stuxnet is believed to have caused material damage to approximately 1000 centrifuges. Therefore, its payload resulted in a significant degree of increased entropy within the Natanz facility. This was also evident from the IAEA's reports demonstrating that there was a sudden drop in the number of centrifuges under

[131] Ibid 49.
[132] Ibid 38–39; Zetter (n 15) 123.
[133] Falliere, Murchu, and Chien (n 10) 49.
[134] Ibid 39.
[135] Ibid 41.
[136] Ibid 42-43.
[137] Ibid.
[138] Albright, Brannan, and Walrond (n 16) 4–5.
[139] Falliere, Murchu, and Chien (n 10) 42–43.
[140] Zetter (n 15) 343.
[141] Falliere, Murchu, and Chien (n 10) 43.
[142] Albright, Brannan, and Walrond (n 16) 6.

vacuum and a rise in the number of cascades with disconnected centrifuges,[143] as well as video footage showing that a similar number of centrifuges were dismantled.[144] In effect, these reports indicated that the Natanz facility was not operating normally and that, given the timing, Stuxnet was the likely cause of these increases in entropy.

5 CONCLUSION

As this analysis of the Stuxnet incident demonstrates, in addition to the physical damage Stuxnet caused to approximately 1000 centrifuges, it also undermined the integrity, or disrupted the operation, of thousands of other entities associated with the functioning of the enrichment facility at Natanz. The harm to most of these entities did not involve physical damage and instead mainly involved the disruption of their proper operation. Stuxnet undermined the integrity of over 100,000 computers around the world and 12,000 of these were within the corporations it used to infect the computers at Natanz. It exploited the interactions between these computers to ultimately access the PLCs used to operate uranium enrichment centrifuges. In this process, it undermined the information exchanges between these entities and altered their properties. While it also caused physical damage to approximately 1000 centrifuges, this was only part of the harm that it caused.

Yet the law, as revealed through the orthodox approach to Article 2(4) and the Stuxnet incident, is largely incapable of recognising the non-material harm caused to these entities. Due to its limited conception of violence, Article 2(4) remains fixated on damage to physical objects or harm to human beings within the notion of force. As a result, had Stuxnet merely disrupted the operation of the centrifuges without causing material damage, it would not have been so widely regarded as a use of force and could be described as a 'legal masterpiece'.[145] This is problematic particularly if it had the same effect of disrupting the operation of the enrichment facility at Natanz, as it would not have constituted a form of violence that is captured by the law and would therefore have fallen outside the scope of what is considered force under Article 2(4). This distinction, which is largely based on whether or not a cyberattack results in material effects, can be seen as artificial and not reflecting the technological context in which the law currently operates.[146] States increasingly rely on ICTs for their proper functioning and are vulnerable to new forms of violence in and through cyberspace that challenge the orthodox account of what constitutes a use of force. As such, for Article 2(4) to retain its relevance in limiting interstate violence, the conception of violence embodied in the notion of force needs to be updated to include serious forms of informational violence. By considering the harm caused to a range of material and non-material entities in terms of entropy, Stuxnet can be seen to have involved both forms of physical and informational violence. Not only did it damage physical hardware, it also disrupted or undermined the integrity of thousands of entities and processes associated with the functioning of the enrichment facility at Natanz. Accordingly, Stuxnet constituted a use of force given the degree of entropy it caused overall, and not simply because it caused physical damage.

However, it is not argued that all cyberattacks causing minimal degrees of informational violence should constitute uses of force. This article has sought to highlight the shortcomings of the notion of violence that underpins the orthodox approach to Article 2(4), and demonstrate how an informational approach offers a different way in which to think about violence and the harm caused by cyberattacks. While each cyberattack incident must be considered on a case-by-case basis,[147] by considering the degree of entropy caused, the analysis becomes less restricted to a need for injury or death, or damage or destruction in the physical world.

---

[143] Ibid 2, 8.
[144] Warrick (n 20).
[145] Ziolkowski (n 80) 147. See also Foltz (n 78) 45; Buchan (n 82) 220.
[146] Georg Kerschischnig also notes that '[t]he strict limitation to physical damage clearly does not reflect the realities of cyberspace.' Georg Kerschischnig, *Cyberthreats and International Law* (Eleven International Publishing, The Hague 2012) 135. See also Michael N. Schmitt, 'The Law of Cyber Warfare: Quo Vadis?' (2014) 25 Stanford Law and Policy Review 269, 299.
[147] The Tallinn Manual criteria are useful in making this assessment. *Tallinn Manual 2.0* (n 59) 334–336. Further, these criteria can be improved by, for example, incorporating into the assessment of when a cyberattack constitutes a use of force a need to consider the degrees of increases in entropy caused by a cyberattack when assessing its 'severity'; and

It has been suggested that adopting this approach could make it easier to establish something as a use of force, which in turn could lower the threshold allowing states to respond in self-defence.[148] Given that the purpose of the law on the use of force is to limit states from using forceful means to solve their disputes and thus minimise interstate violence, it runs counter to this purpose for disruptive but seemingly 'non-violent' cyberattacks to not be considered within this prohibition merely because they lack material effects. However, updating Article 2(4)'s conception of violence does not amount to a lowering of the use of force (or the armed attack) thresholds in existing law. Instead, it provides the conceptual tools for considering the harm caused by cyberattacks against a broader range of entities instead of simply human beings and material objects, and the conceptual grounding for the legal justification for states to respond to serious forms of informational violence where appropriate. For example, a significant cyberattack against a state's stock exchange or critical infrastructure—even without material damage—could qualify as such.[149]

Further, it is possible to argue that existing uncertainty within this area of law is useful to avoid an escalation of violence between states. However, as Michael N. Schmitt has pointed out, uncertainty in the law can itself provide the basis for an 'escalatory spiral' where states have differing beliefs about what activities are prohibited by the law and thus differing beliefs about how they can respond to such activities.[150] As such, updating Article 2(4)'s conception of violence to include serious forms of informational violence within the prohibition can help reduce uncertainty and therefore contribute to the development of normative stability in cyberspace.[151]

Accordingly, this article has demonstrated that an informational approach offers a more in-depth account of the harm caused by Stuxnet and how it did so, and it offers a way to think about violence that is not restricted to a strict separation between a cyberattack's physical and virtual effects. It offers a means through which to rethink Article 2(4)'s anthropocentric and materialist conception of violence, as it provides a framework through which the harm to non-material entities and processes can also be considered within the global infosphere. As states are becoming increasingly dependent on ICTs for their proper functioning, the strict separation between the material and non-material effects of cyberattacks is less useful. The functioning of computer systems and networks can be undermined without need for actual physical damage to hardware components. By adopting a broader conception of violence that does not limit its focus to injury to human beings or damage to physical objects, the harm that cyberattacks cause can be considered more universally, in terms of its impact on the infosphere as a whole.

---

the amount of entities harmed and how important they are to the functioning of a state, when considering a cyberattack's 'invasiveness' and 'measurability'. See also Pagallo, 'Cyber Force' (n 85) 414–415.

[148] We are grateful to one of the anonymous reviewers of this article for making this observation.

[149] This is consistent with the view taken by some of the authors of the Tallinn Manual. See *Tallinn Manual 2.0* (n 59) 342–343.

[150] Michael N. Schmitt, 'Grey Zones in the International Law of Cyberspace' (2017) 42(2) Yale Journal of International Law 1, 21.

[151] Ibid 3–4, 21. As Schmitt argues, 'legal clarity breeds international stability. The brighter the red-lines of international law as applied to cyber activities, the less opportunity States will have to exploit grey zones in ways that create instability.' Ibid 21.