Journal of Conflict & Security Law © Oxford University Press 2012; all rights reserved.
For permissions, please e-mail: journals.permissions@oup.com
doi:10.1093/jcsl/krs014

Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?

Russell Buchan*

Abstract

The legality of cyber attacks is generally approached from the use of force prohibition contained in Article 2(4) UN Charter. In order to constitute an unlawful use of force it is widely accepted that an intervention must produce physical damage. Of course, a cyber attack can cause physical damage and therefore violate Article 2(4). Upon the available evidence, I submit that the deployment of the Stuxnet virus against Iran in 2010 is such an example. However, the issue is that many cyber attacks do not manifest physical damage and are thus not captured by Article 2(4). Contrary to claims in existing cyber war literature, this does not mean that such attacks are lawful. Instead, I argue that where such attacks are coercive in nature they will nevertheless violate the non-intervention principle that is embedded in customary international law. I suggest that the cyber attack against Estonia in 2007 provides a good example of a cyber attack amounting to an unlawful intervention.

1. Introduction

Since the dawn of the 'Information Age'[1] States have become highly dependent upon the use of computer technology in order to effectively regulate their societies.[2] However, as recent events have illustrated, hostile actors have recognized this dependency and have increasingly sought to attack computer servers and the information that they hold.[3]

Such operations are known as cyber attacks.[4] Given both the inherent hostility of cyber attacks and their ability to generate grave destructive effects, it is

* Lecturer in Law, University of Sheffield, Sheffield, UK. Email: r.j.buchan@sheffield.ac.uk.

1 The term 'Information Age' was coined by A Toffler and H Toffler, *The Third Wave* (Bantam 1991).

2 'The information age society is highly dependent on computer and internet connections to accomplish tasks both mundane and critical': V Antolin-Jenkins, 'Defining the Parameters of Cyberwar Operations: Looking for Law in All the Wrong Places?' (2005) 51 Naval L Rev 132.

3 As Joyner and Lotrionte note, 'the technology-intensive Information Age brings with it the opportunities for 'cyber-crime', 'cyber war' or, as more aptly put, the prosecution of 'Information Warfare': C Joyner and C Lotrionte, 'Information Warfare as International Coercion: Elements of a Legal Framework' (2001) 12 EJIL 825, 826.

4 The US government defines the term cyber attack as an operation that is designed 'to disrupt, deny, degrade, or destroy information resident in computers and computer

perhaps unsurprising that cyber attacks have been generally approached from the perspective of the *jus ad bellum*;[5] specifically, can cyber attacks be regarded as an unlawful use of force according to Article 2(4) of the United Nations (UN) Charter?[6]

This has proven to be a difficult question for the international lawyer to answer because of the variety of different consequences that cyber attacks can produce.[7] On the one hand, cyber attacks can cause physical damage comparable to an attack by conventional weapons. For example, a cyber attack can disable an air traffic control system and cause planes to crash or can interfere with and corrupt the operating system of a power station and cause a nuclear meltdown. On the other hand, cyber attacks may not cause any physical damage. Examples include cyber attacks that cause key government websites to crash or that destroy or manipulate important information located on computer servers.

Importantly, and as we shall see, Article 2(4) is an effects-based prohibition. The generally accepted interpretation of Article 2(4) is that only those interventions that produce physical damage will be regarded as an unlawful use of force. Consequently, according to positive international law those cyber attacks that do not produce physical damage will not constitute a violation of Article 2(4).[8] Commentators have therefore suggested that these types of cyber attacks fall outside of the international regulatory framework and there are thus 'scant legal impediments to launching the computer wars of tomorrow'.[9]

The argument runs that the UN Charter was established in the immediate aftermath of the Second World War when the main threat to international peace

networks, or the computer networks themselves': Joint Chief of Staff, Joint Pub 3–13, Joint Doctrine for Information Operations GL-5 (9 October 1998).

5 For a different view, see ME O'Connell, 'Cyber Security without Cyber War' in this volume.

6 Art 2(4) provides that '[a]ll Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations'.

7 '. . . the range of hostile activities that can be carried out over information networks is immense, ranging from malicious hacking and defacement of websites to large-scale destruction of the military or civilian infrastructure that rely on those networks': M Waxman, 'Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)' (2011) 36 The Yale J Intl L 421, 422.

8 'Cyberspace operations for the most part do not meet the criteria for "use of force" as currently defined in international law': Antolin-Jenkins (n 2) 134.

9 M Benetar, 'The Use of Cyber Force: Need for Legal Justification?' (2009) 1 Gottingen J Intl L 375, 377. Hoisington explains that '[d]espite the lethality of cyberwarfare, the practice currently exists in a legal netherworld': M Hoisington, 'Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defense' (2009) 32 Boston College Intl Comparative L Rev 439, 440. After categorizing cyber attacks as either a use of force or an act of coercion Barkham explains that '[t]his distinction is important because the Charter, through Article 2(4), bans the use of force, but acts of coercion do not violate international law because they are not uses of force': J Barkham, 'Information Warfare and International Law on the Use of Force' (2001) 34 NYU J Intl L & Pol 56, 84, fn 112.

and security was represented by professional armies employing conventional weapons. Article 2(4) was therefore devised in order to address this type of force. Quite clearly, Article 2(4) was never intended to address attacks against computer systems or the information resident on them. Article 2(4) is thus considered anachronistic and demonstrates an 'inability'[10] to protect states from new methods of warfare like cyber attacks that do not manifest physical damage.[11]

In the context of cyber attacks, Silver refers to this as the 'unsatisfactory reality' of the situation.[12] However, this reality has caused considerable concern within cyber war scholarship, with commentators pointing out that in the Information Age an attack against computers servers or information located on them can be just as destructive as an attack that produces physical damage. Examples usually offered in this context are cyber attacks that disable a State's military defence network or cripple its financial sector.[13]

In light of this, and with the objective of better protecting State security, cyber war scholars propose reforms to the existing international legal framework.[14] Proposed reforms generally fall into one of two categories.[15] The conventional proposal is that Article 2(4) needs to be subject to an 'interpretive reorientation',[16] dilating its scope in order to encompass cyber attacks which, although not producing physical damage, nevertheless have a destructive impact.[17] More recently, there have been sustained calls that a 'new, comprehensive legal

[10] Barkham (n 9) 112

[11] 'The UN Charter was written before the internet existed and, therefore, cyberwarfare presents a unique challenge to traditional definitions of what constitutes a use of force': Hoisington (n 9) 454. 'The tools for analyzing conventional actions under Article 2(4) do not lend themselves well to IW [information warfare]': Barkham (n 9) 112.

[12] D Silver, 'Computer Network Attack as a Use of Force under Article 2(4)' (2002) 76 Intl L Studies 84, 92.

[13] For a discussion of the magnitude of the threat posed by cyber attacks see W Schwartau, *Information Warfare: Chaos on the Electronic Highway* (Thunder's Mouth Press 1994).

[14] 'Given such realities, international legal rules must be dramatically adapted if new cyberspace technologies are to be regulated, or even managed, in their increasingly pervasive transnational applications': Joyner and Lotrionte (n 3) 826.

[15] 'Either Information Warfare will require an expansion of the application of Article 2(4) definition of the use of force or the international community will need to develop news means of addressing the threat, possibly a treaty': Barkham (n 9) 59.

[16] Waxman (n 7) 437.

[17] In his work on the subject, Schmitt has proposed a new 'normative framework' for determining unlawful uses of force that would include interventions (and specifically cyber attacks) even though they do not produce physical damage: M Schmitt, 'Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework' (1998–99) 37 Columb J Transnatl L 885. For a similar approach see T Morth, 'Considering Our Position: Viewing Information Warfare as a Use of Force Prohibited by Article 2(4) of the U.N. Charter' (1998) 10 Case W Res J Intl L 567.

framework is needed to address cyber attacks'.[18] In particular the call has been for an international treaty, similar to the Outer Space Treaty 1967 or the UN Convention on Law of the Sea 1982, which would regulate the use of computer technology and, specifically, prohibit hostile attacks against computer servers or the information resident on them.[19]

This being said, however, dilation of the term 'force' within Article 2(4) either by way of treaty reform or state practice[20] is unlikely. No reform to the text of the UN Charter has ever been agreed and State practice in the context of applying Article 2(4) to cyber attacks is far from consistent.[21] At least anytime soon, the agreement and implementation of an international treaty also seems unlikely.[22] This notwithstanding, the purpose of this article is to argue that contrary to existing claims the current international legal framework *does not* render state security as vulnerable to cyber attacks as contemporary cyber war scholarship would have us believe. Sure, cyber attacks that do not produce physical damage do not fall within the Article 2(4) prohibition. However, I argue that such cyber attacks are nevertheless regulated by international law. Specifically, I submit that such attacks can still be regarded as unlawful on the basis of the principle of non-intervention that is 'part and parcel' of customary international law.[23]

With these issues in mind, this article is structured as follows. In Section 2 I examine the scope of the non-use of force principle contained in Article 2(4) and apply it to the cyber attacks committed against Estonia in 2007 and Iran in 2010. Specifically, I argue that whilst the cyber attacks committed against Estonia cannot be regarded as an unlawful use of force, on the available evidence it is likely that the deployment of the Stuxnet virus against Iran did constitute a violation of Article 2(4). In Section 3, after determining the nature and scope of the non-intervention principle, I submit that the cyber attacks against Estonia amounted to a violation of the Estonian government's right to non-intervention and thus constituted an internationally wrongful act. The utility of the

[18] O Hathaway and others, 'The Law of Cyber-Attack' (2012) 100 California L Rev 1, 5.

[19] D Brown, 'A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict' (2006) 47 Harvard Intl LJ 179; S Shackelford, 'From Nuclear War to New War: Analogizing Cyber Attacks in International Law' (2009) 27 Berkeley J Intl L 192; Barkham (n 9) 95; O'Connell (n 5) s 4.2.

[20] Art 31(3)(b) of the Vienna Convention on the Law of Treaties 1969 (which provides that when interpreting a treaty term one can take into account 'any subsequent practice in the application of the treaty which establishes an agreement of the parties regarding its interpretation').

[21] Waxman notes that 'major actors have divergent strategic interests that will pull their preferred doctrinal interpretations and aspirations in different directions, impeding formation of a stable international consensus': Waxman (n 7) 425–26.

[22] '[I]t will be difficult to achieve international agreement and to enforce it with respect to cyber-attacks': ibid 425.

[23] *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America)* (Merits) [1986] ICJ Rep 14 para 202.

non-intervention principle to protect States against cyber attacks will thus be borne out. Section 4 will offer some conclusions.

2. International Law and the Use of Force

Since the inception of Article 2(4) there has been debate as to whether this prohibition covers only the use of armed force or whether the prohibition extends more widely to the use of political and economic coercion.[24]

In order to determine the correct interpretation of Article 2(4) the starting point must be the Vienna Convention on the Law of Treaties 1969 (VCLT), which provides the rules on treaty interpretation. Article 31 explains that terms within a treaty must be given their ordinary meaning in light of the purpose and objects of the treaty.[25] Conferring the term 'force' its ordinary meaning would indicate that Article 2(4) is intended to cover all uses of force. Patently, Article 2(4) omits any qualification to the term force. Moreover, it is surely significant that at other points in the UN Charter the term *armed* force is expressly used. For example, the preamble to the UN Charter explains that 'armed force shall not be used, save in the common interest'. In addition, Articles 41–46 provide that the Security Council can employ 'measures not involving the use of armed force' or, if such measures prove inadequate, 'armed force'. Thus, the fact that the framers of the UN Charter were minded to expressly state armed force in certain articles would indicate that the use of the term force without qualification in Article 2(4) means that this prohibition is intended to apply beyond armed force; presumably, to include economic and political force.

This interpretation certainly appears to have merit. However, it is important to recognise that, as required by Article 31(1) VCLT, before a treaty term can be given its ordinary meaning, this meaning must be tested (or verified) against the broader purposes and principles of the treaty. In essence, a treaty term cannot be given its ordinary meaning if that meaning defeats or undermines the treaty's wider purpose and objective.[26] In the context of the current discussion this is extremely important. This is because the UN Charter makes it quite clear that the overriding purpose of the UN is to maintain international peace and security by removing the right of its Member States to use armed force and instead locating it within the collective security system.[27] For example, the

[24] See generally G Tunkin, *Law and Force in the International System* (Progress Publishers 1985).

[25] This article is considered to be reflective of customary international law: *Arbitral Award of 31 July 1989* ['...[a]rticles 31 and 32 of the Vienna Convention on the Law of Treaties ... may in many respects be considered as a codification of existing customary international law ...' [1991] ICJ Rep 69–70, para 48.

[26] A Aust, *Modern Treaty Law and Practice* (CUP 2007) 235.

[27] The exception is art 51 UN Charter, which permits states to use force 'where an armed attack occurs'.

preamble to the Charter (which is considered good ground for discerning the purposes and objectives of a treaty[28]) clearly states that the UN is an organization determined to prevent 'the scourge of war' and that 'armed force shall not be used, save in the common interest'. Consequently, if curtailing the ability of its Member States to use *armed* force is the purpose of the UN, this would indicate that the term force in Article 2(4) should be interpreted to mean armed force.

In light of these observations, it is therefore apparent that there is textual support within the Charter to support an interpretation of Article 2(4) that includes political and economic force on the one hand and an interpretation that is restricted to armed force on the other.[29]

Article 32 VCLT provides that if after the application of Article 31 the meaning of the term or provision is still ambiguous recourse can be had to the preparatory materials of the treaty.[30] This is significant in the context of Article 2(4) because the preparatory materials reveal that the Brazilian delegation proposed that Article 2(4) expressly prohibit 'the threat or use of force and the threat or use of economic measures in any manner inconsistent with the purposes of the Organization'.[31] As is well known, this proposal was vetoed by the drafting committee.[32] As a result, 'the *travaux preparatoires* also reveal that the drafters did not intend to extent the prohibition to economic coercion and political pressures'.[33] Thus, the generally accepted interpretation is that the term force within Article 2(4) is limited to *armed* force.[34]

However, it is still necessary to inquire into the meaning of *armed* force. Clearly, the term 'armed' requires that a weapon be used. Black's Law Dictionary defines 'armed' as meaning '[e]quipped with a weapon' or '[i]nvolving the use of a weapon'.[35] But the question then becomes how this weapon must be used in order for a violation of Article 2(4) to occur.

[28] Art 31(2) VCLT.

[29] As Benetar explains, '[w]e can conclude from this analysis that the wording of article 2(4) is ambiguous to say the least': Benetar (n 9) 383.

[30] This article is also considered to be reflective of customary international law: see n 25.

[31] 6 UNCIO Docs 559 (1945).

[32] 6 UNCIO Docs 334–39, 405, 609 (1945).

[33] M Roscini, 'World Wide Warfare – Jus ad bellum and the Use of Force' (2010) 14 Max Planck Ybk UNL 85, 105.

[34] 'The term does not cover any possible kind of force, but is, according to the correct and prevailing view, limited to armed force': A Randelzhofer, 'Article 2(4)' in B Simma (ed), *The Charter of the United Nations: A Commentary* (OUP 2002) 117. 'Unfortunately, "force" itself is a flexible term. Under modern conditions the threat or use of economic retaliation may be as effective against a weaker state as the threat or use of armed force. But it appears that the prohibition of Article 2(4) is directed exclusively at force in the sense of "armed force"': N Bentwich and A Martin, *A Commentary of the Charter of the United Nations* (Routledge & Paul 1950) 12.

[35] B Garner (ed), *Black's Law Dictionary* (West 2009) 123.

At first, it was generally accepted that armed force required the use of a weapon that produced kinetic force,[36] ie the use of a weapon that had an 'explosive effect with shockwaves and heat'.[37] This approach was later criticized by Brownlie on the basis that it would seemingly exclude the use of chemical, biological and nuclear weapons. Clearly, such weapons do not necessarily result in an explosion that produces shockwaves or heat. In order to ensure that such weapons fell within the use of force prohibition, the definition of Article 2(4) moved away from the requirement of kinetic force and towards the *effects* that the weapon produced. In particular, Brownlie argued that the litmus test for determining whether an unlawful use has been committed is whether the weapon used caused 'destruction to life and property'.[38] This effects-based approach has since gained considerable traction in international legal literature, particularly in the context of cyber war.[39] For example, the National Research Council posits 'death or personal injury to people and destruction of physical property as criteria for the definition of the use of force'.[40] Similarly, in his contribution to cyber war scholarship Dinstein explains that cyber attacks must manifest physical damage in order to be regarded as an unlawful use of force: '[i]t does not matter what specific means – kinetic or electronic – are used to bring it about, but the end result must be that violence occurs or is threatened'.[41]

In light of this, I will now assess the well-known cyber attacks committed against Estonia in 2007 and Iran in 2010 in order to demonstrate the types of cyber attack that constitute an unlawful use of force for the purposes of Article 2(4).

[36] J Bond, *Peacetime Foreign Data Manipulation as One Aspect of Offensive Information Warfare: Questions of Legality under the United Nations Charter Article 2(4)* (US Dept of Commerce, National Technical Information Service 1996) 78.

[37] I Brownlie, *International Law and the Use of Force by States* (Clarendon 1963) 362.

[38] ibid. Note that for Brownlie there was no requirement that the force be deployed by the military. Although cf B Roling, '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 1986) 3 ('It seems obvious to the present writer that the "force" referred to in art 2(4) is military force').

[39] 'This fundamental proscription against the use of interstate force is traditionally regarded as being confined to the use or threat of "armed" force, meaning the possible resort to a violent weapon that inflicts human injury': Joyner and Lotrionte (n 3) at 845.

[40] Committee on Offensive Information Warfare and others, *Technology, Policy Law and Ethics Regarding US Acquisition and Use of Cyberattack Capabilities Report* (National Research Council 2009) 253.

[41] Y Dinstein, *War, Aggression and Self-Defence* (CUP 2010) at 88 (fns omitted). Although cf Sharp who argues that 'any computer attack [perpetrated by a state] that intentionally causes *any destructive effect* within the sovereign territory of another state is an unlawful use of force': WG Sharp Sr, *CyberSpace and the Use of Force* (Ageis Research Corp 1999) 133 (emphasis added).

A. Estonia 2007

In early spring April 2007, the Estonian government declared that it would move a statue of a Russian soldier (known as the Bronze Solider) to a new location on the outskirts of the capital city, Tallinn. The reason for this was because the statue had been erected in order to commemorate Soviet soldiers that had lost their lives whilst defeating Nazi Germany during the Second World War and had been long considered a symbol of foreign occupation. Given the large Russian population living in Estonia, this announcement sparked several days of rioting and looting within Tallinn. In addition, these violent protests were accompanied by cyber attacks against government agencies and private companies (such as media stations and banks). Principally, these attacks took the form of distributed denial of service attacks (DDoS), which is where an Internet web page is subject to so many requests for information that it runs extremely slowly or even crashes completely; the sum effect is that legitimate users are denied access. At first, these DDoS 'were simple, ineptly coordinated and easily mitigated'.[42] However, the DDoS attacks quickly became far more organized and sophisticated. In particular, large botnets were used. A botnet describes a collection of compromised (or high jacked) computers that can then be used without the knowledge of the owner. In the Estonian case, the botnets resulted in approximately 85 000 high jacked computers sending requests for information from Estonian Internet web pages. Unable to deal with the barrage of requests, targeted web pages crashed and went off line.[43] All in all, these attacks lasted approximately three weeks (from 26 April to 19 May). Although the Russian government denied responsibility for these attacks and no definite attribution has ever been made, Estonia maintained that Russia was responsible for these cyber attacks.[44]

The question posed in both the media and academic commentary was whether this type of cyber attack (in particular, DDoS attacks) constituted an unlawful use of force. Undeniably, considerable disruption was caused in Estonia. In the words of the Speaker of the Estonian Parliament:

> When I look at a nuclear explosion and the explosion that happened in our country in May, I see the same thing . . . Like nuclear radiation, cyber war doesn't make you bleed, but it can destroy everything.[45]

[42] E Tikk, K Kaska and L Vihul, *International Cyber Incidents: Legal Considerations* (Cooperative Cyber Defence Centre of Excellence 2010) 19.

[43] For an overview of the cyber attacks against Estonia see NATO's documentary entitled 'Six Colours: War in Cyberspace' at <http://www.nato.int/ebookshop/video/six_colours/SixColours.html> accessed 19 June 2012.

[44] 'Russia Accused of Unleashing Cyberwar to Disable Estonia' *The Guardian* (London, 17 May 2007) at <http://www.guardian.co.uk/world/2007/may/17/topstories3.russia> accessed 8 April 2012.

[45] E Ergma, Speaker of the Estonian Parliament, quoted in J Davis, 'Hackers Take Down the Most Wired Country in Europe' *Wired Magazine* (21 August 2007).

However, the point that this quotation misses is that unlike a nuclear explosion the cyber attacks committed against Estonia did not cause any physical damage,[46] even though the *disruptive* effects may have been comparable with such an attack. This is significant because, as I have explained, a violation of Article 2(4) will only occur where a weapon is used that produces physical damage. To this end, in the absence of physical damage I submit that the cyber attacks committed against Estonia cannot be regarded as an unlawful use of force for the purposes of Article 2(4).

B. Iran 2010

In July 2010 the Iranian government detected a computer malware virus installed in its computer systems. This computer virus has since become known as Stuxnet. Although Stuxnet was discovered in many different computer systems in Iran, the epicentre of the Stuxnet attack was at Natanz nuclear plant.

Natanz is Iran's leading nuclear plant and is used to enrich uranium. The Iranian government maintains that its uranium enrichment programme is pursuant to exclusively peaceful purposes; namely, to produce nuclear power. However, there are acute concerns within the international community that any nuclear material will be used to source weapons of mass destruction.[47]

In order for uranium to be enriched to a sufficient level of purity to produce nuclear material it must be exposed to very precise conditions. The conventional method by which uranium is enriched is by placing it in centrifuges which are then spun at a specific speed and subject to a particular temperature and pressure.

The Stuxnet virus was designed to force a change in the rotor speed of the centrifuges, causing the speed at which they rotate to substantially increase and then to drastically decrease. In order for this to be achieved the virus operated covertly, being able to conceal its presence by informing system operators that the centrifuges were operating normally.[48]

Significantly, the Iranian government has not revealed specific details concerning the impact of the Stuxnet virus. On 23 November 2010 Ali Akbar Salehi, the then Head of Iran's Atomic Energy Organization, explained that '[w]e discovered the virus exactly at the same spot it wanted to penetrate because of our vigilance and prevented the virus from harming [equipment]'.[49] This suggests that the Stuxnet virus had little significant impact at Natanz,

[46] 'No lives were lost, no troops deployed across borders, and no guns were fired . . . [in conclusion] the cyber-assault on Estonia failed to generate physical damage': K Hinkle, 'Countermeasures in the Cyber Context: One More Thing to Worry About' (2011) 37 Yale J Intl L Online 11,13–14.

[47] See SC Res 1696 (31 July 2006).

[48] For a discussion of the Stuxnet virus, see P Shakarian, 'Stuxnet: Cyberwar Revolution in Military Affairs' (2011) 7 Small Wars J 1.

[49] Quoted in 'Iran 'Briefly Halted Enrichment'' *Aljazeera* (23 November 2010).

being detected and removed before it could adversely affect the process of uranium enrichment. In contrast, the Iranian President conceded that some damage was caused but has been coy as to the exact nature: '[t]hey succeeded in creating problems for a limited number of our centrifuges with the software they installed in electronic parts'.[50]

This being said, it is important to recognize that other reports have suggested that the damage caused by Stuxnet was far more severe than the Iranian government has admitted. Clearly, by increasing and decreasing the speed of the centrifuges the uranium resident within those centrifuges could not have been enriched to a level of purity needed to produce nuclear material. However, the Institute for Science and International Security has explained that by increasing and decreasing the speed of rotation, the effect of the Stuxnet virus was to induce excessive vibrations in the centrifuges.[51] The Institute claims that such vibrations could be sufficient to cause the centrifuges to be destroyed. In fact, relying upon evidence made available by the International Atomic Energy Agency, the Institute explains that '[i]n late 2009 or early 2010, Iran decommissioned or replaced about 1,000 IR-1 centrifuges in the Fuel Enrichment Plan (FEP) at Natanz'[52] and that the Stuxnet virus is 'a reasonable explanation for the apparent damage' at Natanz.[53] Putting this into context, experts have suggested that this damage set back Iran's aspirations to enrich uranium by up to two years.[54]

Appreciating that Article 2(4) is an effects-based prohibition, determining whether the attack against Iran amounted to an unlawful use of force is problematic because the exact impact of the Stuxnet virus has never been concretely identified. As I have noted, the President of Iran conceded that Stuxnet had 'caused problems'. If this means that the computer virus prevented the centrifuges from rotating at the correct speed and that this in turn prevented the uranium from being enriched, the Stuxnet attack cannot be regarded as an unlawful use of force because no damage to physical property was caused.[55] However, if reports by the Institute for Science and International Security are

[50] Quoted in 'Iran says Cyber Foes Caused Centrifuge Problems' *Reuters* (29 November 2010).

[51] The Institute produced its Preliminary Report on 22 December 2010: D Albright, P Brannan and C Walrond, 'Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? Institute for Science and International Security' (Institute for Science and International Security, 22 December 2010). This report was updated on 15 February 2011: D Albright, P Brannan and C Walrond, 'Stuxnet Malware and Natanz: Update of ISIS December 22, 2010 Report' (Institute for Science and International Security, 15 February 2011).

[52] ibid (Report of 22 December 2010) 1.

[53] ibid 5.

[54] Y Katz, 'Stuxnet Virus Set Back Iran's Nuclear Program by 2 Years' *Jerusalem Post* (Jerusalem, 15 December 2010) at <http://www.jpost.com/IranianThreat/News/Article.aspx?id=199475> accessed 8 April 2012.

[55] J-C Woltag, 'Computer Network Operations Below the Level of Armed Force' (European Society of International Law Conference Paper Series 1, Tartu, Estonia, 26 May 2011).

correct and the Stuxnet virus did cause the physical destruction of centrifuges at Natanz, this would constitute the requisite physical damage in order for a violation of Article 2(4) to be established.

3. The Principle of Non-intervention

Traditionally, legal appraisal of interventions in the domestic affairs of states has been approached from the use of force perspective.[56] However, as the ICJ noted in the *Nicaragua* case, the use of force is a 'particularly obvious example' of an unlawful intervention.[57] Thus, '[w]hile the customary rules of international law relating to intervention have now to a considerable extent to be considered alongside the more general prohibition on the use of force, intervention is still a distinct concept'.[58] In the words of Judge Jennings, '[t]here can be no doubt that the principle of non-intervention is an autonomous principle of customary law'.[59]

Cyber war scholarship has followed a similar pattern. In examining the legality of cyber attacks many commentators have focused exclusively on Article 2(4), failing to consider the wider customary principle of non-intervention.[60] Whilst others have recognized 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.[61]

The argument pursued in this article is that the non-intervention principle represents a useful legal tool available to States to protect them from cyber attacks which, although not causing physical damage, nevertheless produce deleterious effects. However, before our attention turns to an examination of the principle of non-intervention, it is necessary to briefly consider why this principle has hitherto been given so little attention in cyber war scholarship.

[56] 'Most of the scholarly literature on intervention in internal affairs has focused on forcible forms of influence. Indeed, the prevailing viewpoint until well into the 20th century was that the international legal concept of intervention concerned itself only with the use or threat of force against another state and not with lesser techniques': L Damrosch, 'Politics Across Borders: Nonintervention and Nonforcible Influence of Domestic Affairs' (1989) 83 AJIL 1 at 3 (fns omitted).

[57] *Nicaragua* (n 23) para 205.

[58] R Jennings and A Watts, *Oppenheim's International Law* (Longman 1992) 429.

[59] *Nicaragua* (n 23) 534.

[60] E Kodar, 'Computer Network Attacks in the Grey Areas of Jus ad Bellum and Jus in Bello' (2009) 9 Baltic Ybk Intl L 133; Morth (n 17); E Talbot Jensen, 'Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense' (2002) 38 Stanford J Intl L 207; Barkham (n 9); Hoisington (n 9); Antolin-Jenkins (n 2).

[61] Waxman (n 7); Benatar (n 9); Roscini (n 33); Schmitt (n 17); Joyner and Lotrionte (n 3); Silver (n 12). The exception here is Woltag (n 55), who does give greater consideration to the principle of non-intervention.

The explanation seems to rest upon the definition that has been traditionally ascribed to the legal concept of state sovereignty. In particular, the term state sovereignty has generally been defined by reference to a state's physical territory. In this sense, states have often been understood to possess 'territorial sovereignty';[62] 'sovereignty has always been, in part, based on the idea of territoriality. The extent of a sovereign's reach has usually been decided by geographic borders'.[63] In the words of the ICJ:

> The basic legal concept of State sovereignty in customary international law . . . extends to the internal waters and territorial sea of every State and to the air space above its territory.[64]

Defining state sovereignty in terms of physical territory yields important implications for the scope of the principle of non-intervention, which is considered to be the 'corollary' of the principle of state sovereignty.[65] In essence, the upshot of such a definition is that an unlawful intervention can only occur where the physical territory of a State has been violated.[66]

Bearing this in mind, cyberspace is often regarded as a virtual domain over which no State is able to exercise territorial control. According to the International Humanitarian Law Institute, '[t]he distinctive feature of cyberspace is that it is a notional environment and beyond the jurisdiction of any single nation.'[67]

Instead, the suggestion is that cyberspace is part of the global commons. This is certainly the opinion of the US Department of Defense, which explains that 'the global common consists of international waters and airspace, space and cyberspace'.[68]

[62] 'Between independent States, respect for territorial sovereignty is an essential foundation of international relations': *Corfu Channel (United Kingdom v Albania)* (Merits) [1949] ICJ Rep 4, 35.

[63] W Wriston, *The Twilight of Sovereignty: How the Information Revolution is Changing Our World* (Scribner 1992) 7; '[C]urrent paradigms of international law focus on a state-based structure that is preoccupied with the notions of sovereignty and territory': S Kanuck, 'Recent Development: Information Warfare: New Challenges for Public International Law' (1996) 37 Harvard Intl LJ 272, 286; 'Sovereignty, a fundamental principle of international law since the Treaty of Westphalia of 1648, holds that each state retains exclusive authority over activities within its border': Joyner and Lotrionte (n 3) 843.

[64] *Nicaragua* (n 23) para 212.

[65] ibid para 202.

[66] As the Permanent International Court explained in the *Lotus* case, 'the first and foremost restriction imposed by international law upon a State is that . . . it may not exercise power in any form in the territory of another state. In this sense jurisdiction is certainly territorial. . .': *SS Lotus Case (France v Turkey)* [1927] PCIJ Rep Series A No 10, 18.

[67] International Humanitarian Law Institute, *Rules of Engagement Handbook* (September 2009) 15.

In light of these points, it is unsurprising that commentators have failed to seriously consider whether an unauthorized intervention in the virtual domain of another State can be regarded as an unlawful intervention in a State's sovereignty. For example, in the context of cyber attacks Kanuck explains that 'it hardly seems plausible that one state's interference with an intangible phenomenon such as radiation or electricity constitutes a *per se* legal violation against any particular state'.[69]

However, I argue that the concept of state sovereignty does not only extend to the physical territory of a State; in short, sovereignty transcends notions of territorial control. Instead, I argue that customary international law accords a far wider definition to the term state sovereignty. More generally, I submit that state sovereignty protects from external intervention the decision-making capacity of a state to formulate policies in relation to its internal and external affairs.

This broader understanding of the concept of state sovereignty finds textual support in the jurisprudence of the ICJ. In determining both the customary status of the non-intervention principle and its scope, in the *Nicaragua* case the ICJ determined that:

> A prohibited intervention must . . . be one bearing on matters in which each State is permitted, by the principle of State sovereignty, to decide freely. One of these is the choice of a political, economic, social and cultural system, and the formulation of foreign policy. Intervention is wrongful when it uses methods of coercion in regard to such choices, which must remain free ones . . . the element of coercion . . . defines, and indeed forms the very essence of, prohibited intervention.[70]

Thus, as Jamnejad and Wood explain, 'the essence of intervention is coercion'.[71] It is only those acts that are of sufficient magnitude that will qualify as coercive and therefore fall within the non-intervention principle. In this context, a good

[68] US Department of Defense, *The Strategy for Homeland Defense and Civil Support* (June 2005) 12.

[69] Kanuck (n 63) 288.

[70] *Nicaragua* (n 23) para 205. This definition was based on the General Assembly's Friendly Relations Declaration, which discusses at length the non-intervention principle. The Resolution explains that '[n]o State may use or encourage the use of economic, political or any other type of measures to coerce another State in order to obtain from it the subordination of the exercise of its sovereign rights and to secure from its advantages of any kind': UN Doc A/RES/2625 (XXV).

[71] M Jamnejad and M Wood, 'The Principle of Non-Intervention' (2009) 22 Leiden J Intl L 345, 348. The use of the word coercion is significant because it is clearly boarder than the notion of 'dictatorial interference' that had been traditionally employed in order to determine unlawful interventions: Jennings and Watts (n 58) 418 ('the interference must be forcible or dictatorial, or otherwise coercive, in effect depriving the state intervened against of control over the matter in question'). Although do note Judge Schwebel's dissent in *Nicaragua* where he suggested that the court had erred in applying a weaker standard (coercion) than 'dictatorial interference': *Nicaragua* (n 23) 305.

indicator of sufficient magnitude will be where the act is intended to force a policy change in the target State.[72]

However, it is important to realize that coercion alone does not suffice in order to establish an unlawful intervention. This coercion must be exercised in relation to a matter that the victim State is freely entitled to determine itself; in the words of the ICJ, 'choices which must remain free ones'. This point has been recognized by Damrosch in her seminal work on this topic. She explains that there is 'a rather serious gap between what a broad view of the nonintervention norm would require and what states actually do'.[73] Note that Damrosch is not suggesting that the non-intervention principle has fallen into desuetude. On the contrary, Damrosch accepts that the principle of non-intervention is reflected in positive international law. The point that she is making, however, is that the exercise of coercion by one State against another may not always be prohibited under customary international law. In essence, that through customary practices States can modify the scope of the non-intervention principle. In fact, changes to the scope of the non-intervention principle were expressly considered by the ICJ in the *Nicaragua* case. The ICJ had to determine whether 'there might be indications of practice illustrative of a belief in a kind of general right for States to intervene, directly or indirectly, with or without armed force, in support of the internal opposition in another State, whose cause appeared particularly worthy by reason of the political or moral values with which it is identified'.[74] However, the ICJ observed that even in the limited instances where States had supported internal groups they had 'not justified their conduct by reference to a new right of intervention or a new exception to the principle of its prohibition'.[75] Thus, the ICJ concluded that 'no such general right of intervention, in support of the opposition within another State, exists in contemporary international law'.[76] This notwithstanding, the importance of this dictum is that the ICJ recognized that the scope of the non-intervention principle can be modified where there exists sufficient state practice accompanied by *opinio juris*.

This being said, the purpose of this article is not to engage in a comprehensive review of the principle of non-intervention and to determine its scope under contemporary customary international law. Instead, my objective is to demonstrate that the principle of non-intervention is applicable to cyber attacks, especially those that do not qualify as an unlawful use of force. All in all, in order to establish a violation of the non-intervention principle two questions must be addressed. First, is the intervention intended to force the victim State into a change of policy? It is the intentional application of coercion, as opposed to

[72] 'Only acts of a certain magnitude are likely to qualify as 'coercive', and only those that are intended to force a policy change in the target State will contravene the principle': Jamnejad and Wood (n 71) 348.
[73] Damrosch (n 56) 2.
[74] *Nicaragua* (n 23) para 206.
[75] ibid para 207.
[76] ibid para 209.

mere influence, that the principle of non-intervention proscribes.[77] This will require an assessment of the impact of the intervention on the victim State. Secondly, if the intention to impose coercion is present, it must then be asked whether the application of coercion bears upon matters which a state is entitled to freely determine itself. This will require identification of the purpose for why the coercive act was deployed. If, via customary international law, state practice indicates that the application of this type of coercion is permissible, an unlawful intervention cannot be established.

With this in mind, it is now necessary to determine whether the cyber attacks against Estonia in 2007 can be considered acts of unlawful intervention.[78] First, did the cyber attacks result in the application of coercion against Estonia? Or to put the matter differently, were these cyber attacks committed with the intention of forcing the Estonian government into a policy change?

In order to answer this question it is necessary to identify the extent of the disruption caused by the DDoS attacks in Estonia. In this context it significant that in 2007 Estonia was the 'most wired country in Europe';[79] at that time Estonia was 'an information society'.[80] Thus, when the cyber attacks occurred the government, the private sector and individual citizens were heavily dependent upon Internet services in order to conduct their daily affairs. For example, in 2007 approximately 95% of all banking operations were carried out electronically.[81] Consequently, by causing the websites of many of Estonia's largest banks to crash, the DDoS attacks had a profound disruptive effect on economic activity.

Media stations also came under attack. This is significant because access to media in Estonia is principally achieved through the Internet. Thus, by systematically knocking offline major news websites, the Internet could not be used to communicate information relating to the disruption being caused by the cyber attacks to concerned citizens. Moreover, when it was discovered that the DDoS attacks were emanating from abroad, in order to mitigate the attacks new editors disconnected their external networks, thereby blocking all international web traffic. In essence, Estonia was cut off from the rest of the world.

The impact of the DDoS attacks was just as severe in the public sector, with key government websites being targeted. Of the most important, this included websites run by: the office of the Prime Minister and his political party, the office of the President, the Parliament and the State Audit Office. Furthermore, websites belonging to state agencies such as the Police Board and government

[77] Thus, 'the requirement of coercion properly delimits the principle': Jamnejad and Wood (n 71) 348.

[78] I do not consider whether the deployment of the Stuxnet virus constituted an unlawful intervention. As I have already noted, it is likely that the Stuxnet virus amounted to an unlawful use of force and, on this basis, would be therefore unlawful.

[79] Davis (n 45).

[80] Tikk, Kaska and Vihul (n 42) 16.

[81] ibid 17.

ministries were targeted. Indeed, such was the intensity of these attacks that these websites ceased to function, thereby preventing government officials and citizens from updating or accessing information on these websites and maintaining email contact.[82]

Finally, it is important to note that these cyber attacks against the public and private sector lasted for a period of three weeks. To this end, given the severity of the cyber attacks and their duration, I submit that these attacks 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.

Turning to the second question, did this coercion relate to a matter that the government was entitled to freely decide itself? In essence, this boils down to whether custom has evolved in such a way that now recognizes the right of States to apply coercion against another State where it has decided to relocate memorials of particular significance. Clearly, decisions relating to the location (or relocation) of memorials remains the free choice of any government. In other words, this is a decision within the sovereign domain of national governments and is protected by the principle of non-intervention. To this end, I contend that the cyber attacks against Estonia constituted a violation of Estonia's sovereignty and thus an unlawful intervention.

Importantly, where a violation of the non-intervention occurs the victim State will be able to establish the commission of an internationally wrongful act. This will confer the victim State the legal right to claim cessation of the unlawful act, assurances as to non-repetition and, if appropriate, reparations.[83] Moreover, customary international law will permit the victim State to deploy countermeasures if the unlawful act (the cyber attack) is continuing.[84] Of course, any countermeasures would need to be both proportionate and necessary in the circumstances.[85] In light of the preceding discussion, it therefore becomes apparent 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.

[82] As Woltag explains, 'the effects mainly resonated within the economy and civil society, with business activities relying on an Internet connection impaired due to the breakdown of email and web servers. Sovereign functions such as electronic communication between public authorities and citizens were also disturbed, along with general access to public information complicated. Furthermore, access to domestic and foreign media available on the Internet was hindered, encroaching upon the free flow of information': Woltag (n 55) 5.

[83] See arts 30 and 31 of the International Law Commission's Draft Articles on State Responsibility (2001).

[84] ibid art 49.

[85] ibid art 51.

4. Conclusion

The motivation for this article is based on the concern that cyber war scholarship has focused too heavily upon whether or not a cyber attack amounts to an unlawful use of force under Article 2(4). Sure, a cyber attack that produces physical damage will amount to a violation of Article 2(4). A good example of this is the cyber attack against Iran in 2010. Although there are questions over the exact impact of the Stuxnet virus, the general consensus is that the computer virus physically destroyed centrifuges at Natanz nuclear facility. Such physical damage would bring this attack within the prohibition contained in Article 2(4).

However, it is perfectly conceivable that a cyber attack will not produce physical damage and thus will not violate Article 2(4). Contrary to claims in existing scholarship, this does not mean that such attacks are necessarily lawful. The objective of this article has been to reveal that cyber attacks that do not produce physical damage but do yield damaging effects may still fall foul of the non-intervention principle. As I have argued, a cyber attack will constitute an unlawful intervention under customary international law where it can be regarded as the intentional application of coercion against a State in relation to a matter that it is freely entitled to determine. I submit that the cyber attacks against Estonia in 2007 provide a good example of cyber attacks amounting to an unlawful intervention. It is thus apparent that the principle of non-intervention represents a powerful (albeit often unrecognized) international legal tool that can be used by States in order to protect them from coercive cyber attacks. One final point is necessary. It is important to make it clear that I do not disagree with increasing calls within cyber war literature that an expansion of the term force within Article 2(4) or the implementation of a specific international treaty dealing with the threats posed by computer technology would be beneficial. Rather, the purpose of this article has been to demonstrate that in the absence of such reforms (which, at least anytime soon, seem unlikely), recent criticisms by cyber war scholars that 'existing law is deficient'[86] and that this therefore renders State security vulnerable to violation are misplaced and based upon an inchoate reading of international law.

[86] Hathaway and others (n 18) 5.