Radosław Fordoński
Uniwersytet Warmińsko-Mazurski w Olsztynie
ORCID: 0000-0001-8127-5986

Wojciech Kasprzak
ORCID: 0000-0003-3683-7825

WannaCry ransomware cyberattack as violation of international law

Introduction

On 12 May 2017, a ransomware[1] attack called "*WannaCry*" began affecting computers around the globe. It affected between 230,000 and 300,000 machines in over 150 countries by encrypting computer files and demanding $300 in crypto currency from users in order to restore access. The operation exploited a software vulnerability in systems running older versions of Microsoft Windows that had not installed up-to-date security patches.

[1] Ransomware is a type of malware that prevents or limits users accessing their system, either by locking the system's screen or by locking the users' files unless a ransom is paid. See European Commission, Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, EU Doc JOIN(2017) 450 final, 13 September 2017, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017JC0450&from=EN (accessed 7 July 2018), 2. Compare the definition of the European Union Agency for Law Enforcement Cooperation (Europol): "Ransomware is malware that prevents or limits users from accessing their systems or devices, demanding they pay a ransom, using certain online payment methods and by a set deadline, in order to regain control of their data.") See European Union Agency for Law Enforcement Cooperation, 'Wannacry Ransomware', May 2017, available at: https://www.europol.europa.eu/wannacry-ransomware (accessed 19 September 2018). See also definition produced by the US Federal Bureau of Investigation in a June 2017 document filed in the federal District Court for the Central Disctrict of California: "Ransomware is a type of malware that infects a computer and encrypts some or all of the data or files on the computer, and then demands that the user of the computer pay a ransom in order to decrypt and recover the files, or in order to prevent the malicious actors from distributing the data.") See *United States of America v. Park Jin Hyok*, Criminal Complaint of 8 June 2018, available at: https://www.justice.gov/opa/press-release/file/1092091/download (accessed 17 September 2018), para. 31. See also 'Cyber-attack glossary: What are malware, patches and worms?', BBC News online edition, 15 May 2017, available at: https://www.bbc.co.uk/news/technology-39928596 (accessed 12 September 2018) ("Ransomware ia a program that scrambles a computer's files, demanding payment before they can be opened again.").

Nissan Motor Manufacturing UK in Tyne and Wear, England, halted production after the ransomware infected some of their systems. Renault also stopped production at several sites in France in an attempt to stop the spread of the ransomware. Spain's Telefónica, FedEx and Deutsche Bahn were hit, along with many other countries and companies worldwide[2]. In Brazil, the social security system had to disconnect its computers and cancel public access. The state-owned oil company Petrobras and Brazil's Foreign Ministry also disconnected computers as a precautionary measure, and court systems went down, too[3].

Hardest hit, however, was England's National Health Service (NHS England).

According to information provided to the FBI by the United Kingdom's National Crime Agency, at least 80 out of 236 NHS trusts (organizations serving a particular function or geographic area) across England were affected either because they were infected or because they had to disconnect as a precaution; at least 37 NHS "trusts" were in fact infected with *WannaCry*. An additional 603 primary care or other NHS organizations were infected. National coordination was undertaken during this major incident and remedial action was taken by local organizations to address the vulnerability and the spread of the malware to prevent further infections. There was no patient harm reported during the incident, but the effects included 6,912 appointments that were cancelled (and subsequently re-scheduled) between 12 and 18 May 2017, and 1,220 (approximately 1%) pieces of diagnostic equipment across the NHS that were affected by *WannaCry*. No NHS organizations paid the ransom, consistent with advice not to do so that was given by NHS during the incident[4].

In sum, Europol called the *WannaCry* the "largest ransomware attack observed in history"[5]. There was "no precedent for a ransomware attack of this kind of scale (...) that has been able to attack computers directly with this kind of success."[6] These hackers "have caused enormous amounts of

---

[2] R. Cellan-Jones, 'Ransomware and the NHS – the inquest begins', BBC News online edition, 15 May 2017, available at: https://www.bbc.com/news/technology-39917278 (accessed 2 August 2018).

[3] 'Global 'WannaCry' ransomware cyberattack seeks cash for data', Inquirer online edition, 14 May 2017, available at: http://technology.inquirer.net/62579/global-wannacry-ransomware-cyberattack-seeks-cash-data (accessed 2 August 2018).

[4] *US v. Park Jin Hyok*, *supra* note, para. 225. See also M. Schmitt and S. Fahey, 'WannaCry and the International Law of Cyberspace', Just Security online edition, 22 December 2017, available at: https://www.justsecurity.org/50038/wannacry-international-law-cyberspace/ (accessed 9 September 2018).

[5] 'NHS cyber-attack: No 'second spike' but disruption continues', BBC News online edition, 15 May 2017, available at: https://www.bbc.com/news/uk-39918426 (accessed 2 August 2018).

[6] J. Berr, "WannaCry" ransomware attack losses could reach $4 billion', CBS News online edition, 16 May 2017, available at: https://www.cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses/ (accessed 2 August 2018) (quoting Matthew Anthony, vice president of incident response at security firm Herjavec Group).

disruption", said Graham Cluley, a veteran of the anti-virus industry in Oxford[7].

Concerning a question of attribition of the May 2017 cyberattack, the US administration formally accused the government of the *Democratic* People's *Republic of Korea* of responsibility for the *WannaCry* in December 2017. The accusation came first in a *Wall Street Journal* op-ed by U.S. Homeland Security Advisor Tom Bossert on 18 December. "North Korea has acted especially badly, largely unchecked, for more than a decade, and its malicious behaviour is growing more egregious. WannaCry was indiscriminately reckless", Bossert wrote. "As we make the internet safer, we will continue to hold accountable those who harm or threaten us, whether they act alone or on behalf of criminal organisations or hostile nations", he went on. "The tool kits of totalitarian regimes are too threatening to ignore."

At a press briefing on the following day, Bossert explained that North Korea's "malicious behavior is growing more egregious, and . . . [t]he attribution is a step towards holding them accountable. (...) We do not make this allegation lightly. We do so with evidence, and we do so with partners. Other governments and private companies agree. The United Kingdom, Australia, Canada, New Zealand, and Japan have seen our analysis, and they join us in denouncing North Korea for WannaCry."[8]

On the very same day, the UK Foreign Office Minister for Cyber Lord Ahmad of Wimbledon has also attributed the *WannaCry* ransomware incident to the North Korean *Lazarus* Group[9].

The attribution is in many ways unsurprising. Private companies alleged North Korean involvement within days of the ransomware's

---

[7] 'Global 'WannaCry' ransomware cyberattack seeks cash for data', *supra* note 3.

[8] K. Eichensehr, 'Three Questions on the WannaCry Attribution to North Korea', Just Security, 20 December 2017, available at: https://www.justsecurity.org/49889/questions-wannacry-attribution-north-korea/ (accessed 9 July 2018); 'Cyber-attack: US and UK blame North Korea for WannaCry', BBC News online edition, 19 December 2017, available at: https://www.bbc.com/news/world-us-canada-42407488 (accessed 2 August 2018).

[9] 'Foreign Office Minister condemns North Korean actor for WannaCry attacks', 19 December 2017, available at: https://www.gov.uk/government/news/foreign-office-minister-condemns-north-korean-actor-for-wannacry-attacks (accessed 2 August 2018) ("The UK's National Cyber Security Centre assesses it is highly likely that North Korean actors known as the Lazarus Group were behind the WannaCry ransomware campaign – one of the most significant to hit the UK in terms of scale and disruption. We condemn these actions and commit ourselves to working with all responsible states to combat destructive criminal use of cyber space. The indiscriminate use of the WannaCry ransomware demonstrates North Korean actors using their cyber programme to circumvent sanctions. International law applies online as it does offline. The United Kingdom is determined to identify, pursue and respond to malicious cyber activity regardless of where it originates, imposing costs on those who wish to attack us in cyberspace. We are committed to strengthening coordinated international efforts to uphold a free, open, peaceful and secure cyberspace. The decision to publicly attribute this incident sends a clear message that the UK and its allies will not tolerate malicious cyber activity.").

spread[10]. Microsoft president Brad Smith also expressed his belief that North Korea was behind the May 2017 cyberattack. Smith told British ITV News in October 2017 that at this point "all observers in the know" concluded that North Korea was behind the attack.[11] Also in October 2017, Home Office Minister Ben Wallace told BBC Radio 4's Today programme that the government was "as sure as possible" that North Korea was behind the attack: "This attack, we believe quite strongly that it came from a foreign state. It is widely believed in the community and across a number of countries that North Korea [took on] this role."[12]

North Korea called the accusations "groundless speculation". A spokesman for the North's Korea-Europe Association called the UK's accusation "a wicked attempt" to tighten international sanctions on the country. "This is an act beyond the limit of our tolerance and it makes us question the real purpose behind the UK's move", he said in comments carried on the Korean Central News Agency on 31 October 2017[13].

Political claims of Pyongyang's responsibility were supported credibly, however, by a detailed technical analysis offered by the FBI in the affidavit filed against the *Lazarus* group hacker, Park Jin Hyok, in June 2018[14].

Nonetheless, the attribution raises two important questions.

First, Bossert's December 2017 statements involved endorsement of countermeasures taken by private corporations in response to hostile acts of the State. In the 18 December 2017 *Wall Street Journal* piece, Mr Bossert said North Korea must be held "accountable" and that the US would continue to use a "maximum pressure strategy" to hinder the regime's ability to mount cyber-attacks. Interestingly, although Bossert announced no governmental action besides the attribution itself, he praised the actions of private companies. He said, "We call on the private sector to increase its accountabil-

---

[10] G. Corera, 'NHS cyber-attack was 'launched from North Korea", BBC News online edition, 16 June 2017, available at: https://www.bbc.co.uk/news/technology-40297493 (accessed 2 August 2018) (stating that "Adrian Nish, who leads the cyber threat intelligence team at BAE Systems, saw overlaps with previous code developed by the Lazarus group: "It seems to tie back to the same code-base and the same authors. The code-overlaps are significant.""). See also *US v. Park Jin Hyok*, *supra* note, para. 229 (noting that Symantec also reported that the WannaCry ransomware was linked to the *Lazarus* group).

[11] R. King, 'Microsoft head blames North Korea for ‚WannaCry' hospital cyberattack', Washington Examiner online edition, 14 October 2017, available at: https://www.washingtonexaminer.com/microsoft-head-blames-north-korea-for-wannacry-hospital-cyberattack/article/2637533 (accessed 9 July 2018).

[12] 'NHS ‚could have prevented' WannaCry ransomware attack', BBC News online edition, 27 October 2017, available at: https://www.bbc.co.uk/news/technology-41753022 (accessed 2 August 2018).

[13] 'North Korea calls UK WannaCry accusations 'wicked", BBC News online edition, 31 October 2017, available at: https://www.bbc.co.uk/news/world-asia-41816958 (accessed 2 August 2018).

[14] *US v. Park Jin Hyok*, *supra* note 4, paras. 230–244.

ity in the cyber realm by taking actions that deny North Korea and other bad actors the ability to launch reckless and destructive cyberattacks. We applaud our corporate partners, Microsoft and Facebook especially, for acting on their own initiative last week without any direction by the U.S. government or coordination to disrupt the activities of North Korean hackers. Microsoft acted before the attack in ways that spared many U.S. targets."[15]

Bossert appeared to reference recent defensive cyber actions by Microsoft that, along with action by Facebook, eliminated certain accounts or profiles believed to be used by North Korean hackers. Later on the same day, 19 December 2017, Microsoft issued a statement, saying that in the preceding week the company "working together with Facebook and others in the security community, took strong steps to protect our customers and the internet from ongoing attacks by an advanced persistent threat actor known to us as ZINC, also known as the Lazarus Group." The statement went on to claim that "[a]mong other steps, last week we helped disrupt the malware this group relies on, cleaned customers' infected computers, disabled accounts being used to pursue cyber-attacks and strengthened Windows defences to prevent reinfection."[16]

Meanwhile, countermeasures are responses by a State to the unlawful cyber operations of, or attributable to, another State that would be unlawful themselves but for the latter's conduct[17]. In other words, as only cyberoperations attributable to States violate the sovereignty of other States, the array of responses provided for in international law with respect to malicious or harmful cyber operations is likewise reserved to States. Private entities enjoy no right under international law to conduct countermeasures or engage in cyberoperations pursuant to the right of self-defense[18]. Recall in this context the 2014 Sony Pictures Entertainment hack that has been attributed to North Korea. The cyberoperation damaged corporate cyberinfrastructure, and, because the operation was conducted by a State, violated US sovereign-

---

[15] Eichensehr, 'Three Questions on the WannaCry Attribution to North Korea', *supra* note 8.

[16] 'Cyber-attack: US and UK blame North Korea for WannaCry', BBC News online edition, 19 December 2017, available at: https://www.bbc.com/news/world-us-canada-42407488 (accessed 2 August 2018). / 'Cyber-attack: US and UK blame North Korea for WannaCry', *supra* note.

[17] M. N. Schmitt, 'Peacetime Cyber Responses and Wartime Cyber Operations Under International Law: An Analytical *Vade Mecum*', (2017) 8 Harvard NSJ (Harvard National Security Journal) 239–282, 253. See also 'Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries', (2001) II (2) YBILC (Yearbook of the International Law Commission) 31–143, 75, commentary to Article 22, para. 1 ("n certain circumstances, the commission by one State of an internationally wrongful act may justify another State injured by that act in taking non-forcible countermeasures in order to procure its cessation and to achieve reparation for the injury.").

[18] Schmitt, 'Peacetime Cyber Responses', *supra* note 17, 253. See also M. N. Schmitt and S. Watts, 'Beyond State-Centrism: International Law and Non-state Actors in Cyberspace', (2016) 21(3) JCSL (Journal of Conflict & Security Law) 595–611, 606 ("Non-state actors may not take countermeasures; such measures are a response reserved to states.").

ty. Yet the company enjoyed no independent right to hack-back against North Korea[19] and was obliged to look to a State authorized to conduct countermeasures under the law of state responsibility. On the other hand, there is no bar to the State in turn authorizing the company concerned, or another non-State actor, to conduct the countermeasure on its behalf[20].

Second, governments involved in the affair missed an opportunity to clarify the bounds of international law in cyberspace. The US statements strongly condemned North Korea's actions, but did not clarify whether the United States regards them as a violation of international law.[21] Bossert's 18 December 2017 op-ed, for example, spoke in terms of "bad behavior." Such language "may be good enough for an op-ed, but these vague, undefined terms continue to fill altogether too many of the cyber discussions in the White House and Congress" and "left [the public] to wonder what the full implications of this cyberattack may have been as a matter of law."[22]

The UK Foreign Office Minister for Cyber, Lord Ahmad of Wimbledon issued a similar condemnation and said "[i]nternational law applies online as it does offline." But he stopped short of saying that *WannaCry* violated international law[23].

Finally, the Council of the European Union "firmly condemn[ed] the malicious use of information and communications technologies (ICTs), including in *Wannacry* and *NotPetya*, which have caused significant damage and economic loss in the EU and beyond. Such incidents are destabilizing cyberspace as well as the physical world as they can be easily misperceived and could trigger cascading events."[24]

---

[19] Schmitt, 'Peacetime Cyber Responses', *supra* note 17, 253.

[20] Schmitt and Watts, 'International Law and Non-state Actors in Cyberspace', *supra* note 18, 606.

[21] Eichensehr, 'Three Questions on the WannaCry Attribution to North Korea', *supra* note 8.

[22] M. J. Adams and M. Reiss, 'How Should International Law Treat Cyberattacks like WannaCry?', Lawfare, 22 December 2017, available at: https://www.lawfareblog.com/how-should-international-law-treat-cyberattacks-wannacry (accessed 9 July 2018). But see Y. Raj, 'US, UK, Japan others accuse North Korea of WannaCry cyberattack', Hindustan Times online edition, 19 December 2017, available at: https://www.hindustantimes.com/world-news/us-uk-japan-others-accuse-north-korea-of-wannacry-cyberattack/story-PQXCs7I8RxUDni8kWhE33O.html (accessed 16 September 2018) (noting that Bossert also used the term "cyber malfeasance"). The word "malfeasance" means "an example of dishonest and illegal behaviour, especially by a person in authority". See 'Malfeasance', Cambridge Dictionary online edition, available at: https://dictionary.cambridge.org/dictionary/english/malfeasance (accessed 19 September 2018).

[23] 'Foreign Office Minister condemns North Korean actor for WannaCry attacks', *supra* note 9.

[24] Council of the European Union, Council Conclusions on malicious cyber activities, EU Doc 7925/18, 16 April 2018, available at: http://data.consilium.europa.eu/doc/document/ST-7925-2018-INIT/en/pdf (accessed 6 July 2018), 2. See also European Commission, Commissioner King's keynote speech at the, ‚WannaCry again? Making our businesses digitally great and cyberproof' conference, Munich, 15 February 2018', 15 February 2018, available at: https://ec.europa.eu/commission/commissioners/2014-2019/king/announcements/commissioner-kings-keynote-speech-

Commenting on the related political statements, Eichensehr stated even that "[t]he silence on the international law questions could mean that governments do not think that there was an international law violation."[25] Such conclusion goes too far, though. According to researchers of the NATO Cooperative Cyber Defence Centre of Excellence Law and Policy Branch, "the WannaCry campaign would not reach the threshold of armed attack or use of force, nor could it be qualified as prohibited intervention, due to the lack of a coercive element with respect to a government. However, government systems were also affected by the operation (Russian Ministry of Interior systems were compromised), which could be considered as interference with 'inherently governmental functions'. This would be a violation of sovereignty, and consequently an internationally wrongful act (...). As for non-government systems, the question of violation of sovereignty is not so clear-cut according to the Tallinn Manual 2.0, but if the ransomware disables systems in what is generally described as 'critical infrastructure', states might explore the option to invoke a violation of sovereignty."[26]

The following analysis verifies the NATO legal analysis of the *WannaCry* cyberattack. It addresses the legality of the May 2017 ransomware from the perspective of three relevant principles of international law, mentioned in the quoted legal opinion: *principle* of State sovereignty, *principle* of non-intervention in in the internal or external affairs of any other State and, finally, prohibition of use of force in international relations.

1. *WannaCry* as a violation of State sovereignty

Of all international law principles, sovereignty is perhaps the most fundamental. From that principle emerges, inter alia, notions of noninterven-

---

-wannacry-again-making-our-businesses-digitally-great-and_en (accessed 8 July 2018) ("Last year, the *WannaCry* malware did not just cause computers to freeze, but hospitals to close. It brought the issue of cyber resilience into the mainstream of public and political discourse."); European Commission, Commissioner King's speech at the EU Cybersecurity Conference „Digital Single Market, Common Digital Security 2017", 15 September 2017, in Tallinn, Estonia, 15 September 2017, available at: https://ec.europa.eu/commission/commissioners/2014-2019/king/announcements/commissioner-kings-speech-eu-cybersecurity-conference-digital-single-market-common-digital-security_en (accessed 7 July 2018) ("Since 2016 more than 4,000 ransomware attacks have occurred every day, a 300% increase compared to 2015. Recent big attacks like *WannaCry* showed both how large the impact can be – and how far we have to go in improving our response. It (...) was a powerful reminder of just how significant the challenge facing us is.");

[25] Eichensehr, 'Three Questions on the WannaCry Attribution to North Korea', *supra* note 8.

[26] NATO Cooperative Cyber Defence Centre of Excellence, 'WannaCry Campaign: Potential State Involvement Could Have Serious Consequences', 16 May 2017, available at: https://ccdcoe.org/wannacry-campaign-potential-state-involvement-could-have-serious-consequences.html (accessed 9 July 2018).

tion; prescriptive, enforcement, and adjudicative jurisdiction; sovereign immunity; due diligence; and territorial integrity.[27]

Max Huber set forth the classic definition of sovereignty in his 1928 *Island of Palmas* arbitral award: "Sovereignty in the relations between States signifies independence. Independence in regard to a portion of the globe is the right to exercise therein, to the exclusion of any other State, the functions of a State."[28]

The 1928 *Island of Palmas* arbitration definition signals the two critical aspects of sovereignty: territoriality and State functions. Concerning the former, it is well-accepted that a State's non-consensual, physical penetration of another State's territory, or even unconsented to and adverse presence thereon, amounts to a violation of sovereignty[29].

Regarding the latter, sovereignty has both an internal and external component.

Internal sovereignty refers to the right of a State to exercise its control over persons, including legal persons, objects, and activities on its territory. It is incontrovertible that this right extends to control over individuals engaged in cyber activities, cyberinfrastructure located on a State's territory, and any activities in cyberspace that occur in or through that territory[30].

External sovereignty, by contrast, refers to the right of States to engage in international relations, as in the case of conducting diplomacy and entering into international agreements.[31] For example, in the exercise of external sovereignty a State is free to, or not to, become Party to a treaty governing cyberactivities. Such sovereignty is also the basis for the legal immunity of States[32].

Now, the question is when should a remotely conducted cyber operation by, or attributable to, one State that manifests on cyber infrastructure in

---

[27] M. N. Schmitt, 'Grey Zones in the International Law of Cyberspace', (2017) 42(2) Yale JIL (Yale Journal of International Law) 1–21, 4.

[28] Permanent Court of Arbitration, *Island of Palmas* (*Netherlands v. United States*), Judgment of 4 April 1928, (1928) 2 RIAA (Reports of International Arbitral Awards) 829–871, 838) ("The development of the national organisation of States during the last few centuries and, as a corollary, the development of international law, have established this principle of the exclusive competence of the State in regard to its own territory in such a way as to make it the point of departure in settling most questions that concern international relations.").

[29] M.N. Schmitt, "Virtual' Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law', (2018) 19(1) Chicago JIL (Chicago Journal of International Law) 30–67, 43.

[30] *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations Prepared by the International Groups of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence* (Cambridge/New York: Cambridge University Press, 2017), pp. 13–16. The term "cyberinfrastructure" as used in this Essay refers to "[t]he communications, storage, and computing devices upon which information systems are built and operate." See ibid., p. 564.

[31] Ibid., pp. 16–17.

[32] Ibid., pp. 71–74.

another's territory be treated as analogously running afoul of the obligation to respect the sovereignty of other States.

Experts participating in the Tallinn Manual 2.0 study, representing only the views of the International Group of Experts, but not of NATO, the NATO NATO Cooperative Cyber Defence Centre of Excellence, its sponsoring nations, nor any other State or organization,[33] agreed, based on the right of a State to control access to its territory, that a violation of sovereignty may result from an infringement on a State's territorial integrity. In this regard, they generally agreed that a remotely conducted cyber operation causing physical damage either to the targeted cyberinfrastructure or objects reliant thereon, or injury to persons, violates sovereignty.[34] It makes no difference whether the damaged cyber infrastructure is private or governmental, for the crux of the violation is the causation of consequences upon the State's territory[35].

Furthermore, the *Tallinn Manual 2.0* extended the notion of damage to loss of functionality on the basis that it should not matter whether targeted systems are physically damaged or simply rendered inoperative, for the effect is usually the same the system no longer works. Among the activities proffered by one or more of them as sovereignty violations were: "a cyber operation causing cyber infrastructure or programs to operate differently; altering or deleting data stored in cyber infrastructure without causing physical or functional consequences, as described above; emplacing malware into a system; installing backdoors; and causing a temporary, but significant, loss of functionality, as in the case of a major DDoS operation."[36]

While treating the loss of functionality as the equivalent of physical damage comports with the object and purpose of the rule of sovereignty – to afford the territorial State control over consequential activities on its territory – the *Tallinn Manual 2.0* experts could not achieve consensus as to the precise meaning of "loss of functionality." For some, the notion implies an irreversible loss of function. For others, it extends to situations in which physical repair, as in replacement of a hard drive, is necessary. A number of *Tallinn Manual 2.0* experts would treat the need to replace the operating system or bespoke data upon which the functioning of the system relies as a loss of functionality[37].

---

[33] The *Tallinn Manual 2.0* organizes the rules of international law applying in cyberspace, which were adopted unanimously by an International Group of Experts (IGE) and represent *lex lata*, the law as (those experts believe) it is, as opposed *to lex ferenda*, the law as it ought to be. Ibid., pp. 2–3.

[34] Ibid., p. 20.

[35] Schmitt, "Virtual' Disenfranchisement', *supra* note 29, 43.

[36] *Tallinn Manual 2.0*, *supra* note 30, p. 21.

[37] Ibid. See also Schmitt, "Virtual' Disenfranchisement', *supra* note 29, 44.

Be that as it may, the *WannaCry* cyberattack should be qualified as operation rendering cyberinfrastructure incapable of performing its functions in the manner intended and accordingly as a violation of sovereignty of the affected States.

2. *WannaCry* as a prohibited intervention

Intervention into the internal or external affairs of other States is an internationally wrongful act.[38] Although non-intervention is not explicitly mentioned in the Charter of the United Nations, Article 2(1) acknowledges that the UN is founded on "the principle of the sovereign equality of all its Members",[39] and Article 2(7) clarifies that the Charter does not authorize the UN to "intervene in matters which are essentially within the domestic jurisdiction of any state."[40]

The UN General Assembly further attempted to establish guiding rules on non-intervention in its Declaration on Friendly Relations, which provides that "[n]o State or group of States has the right to intervene, directly or indirectly, for any reason whatever, in the internal or external affairs of any other State"[41] and that "armed intervention and all other forms of interference or attempted threats against the personality of the State or against its political, economic and cultural elements, are in violation of international law."[42]

The 1970 Declaration provides a few concrete examples of intervention, including the organization and encouragement of irregular armed forces and assisting or instigating acts of civil strife or terrorism: "No 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 it advantages of any kind. Also, no State shall organize, assist, foment, finance, incite or tolerate subversive, terrorist or armed activities directed towards the violent overthrow of the regime of another State, or interfere in civil strife in another State."[43]

Most importantly, however, the Declaration on Principles of International Law proclaims that "[e]very State has an inalienable right to choose its

---

[38] *Tallinn Manual 2.0*, *supra* note 30, p. 312.

[39] Charter of the United Nations and Statute of the International Court of Justice, 26 June 1945, 1 UNTS 16, Art. 2(1).

[40] Ibid., Art. 2(7).

[41] GA Res. 2625 (XXV), Declaration on Principles of International Law Concerning Friendly Relations and Co-operation among States in Accordance with the Charter of the United Nations, 24 October 1970, Annex, Principle 3.

[42] Ibid.

[43] Ibid.

political, economic, social and cultural systems, without interference in any form by another State."[44]

The principle of non-intervention applies to cyberspace and information technologies and, as such, it was incorporated into the rules of responsible behavior in cyberspace by UN Group of Governmental Experts. The 2015 Report provides that "it is of central importance" that "in their use of [information and communication technologies], States must observe (...) non-intervention in the internal affairs of other States."[45]

Russia, China, and four other States have gone further by drafting and signing an additional non-binding "international code of conduct for information security."[46]

Intervention was not mentioned in the code, but these States pledged "not to use information (...) to interfere in the affairs of other States or with the aim of undermining [their] political, economic, and social stability."[47]

The "prohibition of intervention" chapter of the *Tallinn Manual 2.0 manual* begins with Rule 66, stating that "[a] State may not intervene, including by cyber means, in the internal or external affairs of another State."[48] The Manual notes that to be prohibited, the intervention must be related to internal or external affairs of a state, it must be coercive,[49] and that even the mere threat of a future intervention violates the norm[50].

The second basis upon which the Experts determined a violation of principle of non-intervention occurs is "when one State's cyber operation interferes with or usurps the inherently governmental functions of another State. This is because the target State enjoys the exclusive right to perform them, or to decide upon their performance. It matters not whether physical damage, injury, or loss of functionality has resulted or whether the operation qualifies in accordance with the various differing positions outlined above for operations that do not result in a loss of functionality."[51]

Put succinctly, an unlawful intervention occurs when (1) the action is

---

[44] Ibid.

[45] Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc A/70/174, 22 July 2015, available at: https://ccdcoe.org/sites/default/files/documents/UN-150722-GGEReport2015.pdf (accessed 20 August 2018), para. 26. See also *ibid*., para. 28 (b) ("*In their use of ICTs, States must observe, among other principles of international law, State sovereignty, sovereign equality, the settlement of disputes by peaceful means and non-intervention in the internal affairs of other States.")*.

[46] International code of conduct for information security, UN Doc A/69/723, 13 January 2015, available at: https://ccdcoe.org/sites/default/files/documents/UN-150113-CodeOfConduct.pdf (accessed 20 August 2018), Annex.

[47] Ibid., para. 2(3).

[48] Tallinn Manual 2.0, supra note 30, p. 312.

[49] Ibid.

[50] Ibid., p. 322.

[51] Ibid., pp. 21–22.

directed at the *domaine réservé* (the internal affairs having to do with the sovereignty) of another State and (2) the action is coercive in nature.

The following analysis will determine existence of both elements in the *WannaCry* cyberattack.

2.1. *WannaCry* as coercion

The International Court of Justice emphasized the centrality of coercion to the notion of non-intervention when it held that "intervention is wrongful when it uses methods of coercion."[52]

The requirement is the essence of intervention, yet it is immensely difficult to define the boundary between coercive and non-coercive actions. International law has never officially defined "coercion," nor does it provide any guidance on how this concept is to be construed in cyberspace operations[53].

According to a classical view, to constitute a violation of international law intervention must be "forcible or dictatorial, or otherwise coercive, in effect depriving the state intervened against of control over the matter in question."[54] An indication of coercion could be that the targeted state is undertaking action that "cannot be terminated at the pleasure of the state that is subject to the intervention."[55] Accordingly, a contemporary commentator defines coercion as an act of a State against another state to compel the latter "to think or act in a certain way by applying various kinds of pressure, threats, intimidation or the use of force."[56]

The *WannaCry* cyberattack does not represent such understanding of the concept of coercion as the latter indicates that the intervening act must be "designed to influence outcomes in, or conduct with respect to, a matter reserved to a target State."[57] Meanwhile the *WannaCry* was a financially motivated attack targeting a private sector.

Being one of the world's most impoverished regimes – with official econ-

---

[52] *Case concerning military and paramilitary activities in and against Nicaragua* (*Nicaragua v. United States of America*) (Merits), Judgment of 27 June 1986 (Merits), ICJ Rep 1986, 14, para. 205.

[53] I. Kilovaty, 'Doxfare: Politically Motivated Leaks and the Future of the Norm on Non-Intervention in the Era of Weaponized Information', (2018) 9 Harvard NSJ (Harvard National Security Journal) 146–179, 168.

[54] R. Jennings and A. Watts, *Oppenheim's International Law* (London/New York: Longman, 2008), Vol. I, p. 432.

[55] E. Dickinson, *The equality of states in international law* (Cambridge: Harvard University Press, 1920), p. 260.

[56] C. C. Joyner, 'Coercion', Max Planck Encyclopedia of Public International Law online edition, December 2006, available at: http://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1749?rskey=qaZy3x&result=1&prd=EPIL (accessed 22 September 2018), para. 1.

[57] *Tallinn Manual 2.0*, *supra* note 30, p. 318.

omy worth $28.4 billion in 2014, according to South Korea's central bank[58] – and facing the toughest and most comprehensive sanctions regime ever imposed by the UN Security Council,[59] Pyongyang has still invested an estimated $1.1 billion to $3.2 billion in the following years toward developing a nuclear deterrent.[60] Accordingly, alleged hacking attempts by North Korea, traditionally intended to cause social disruption or steal classified military or government data, have shifted their focus in recent years to raising foreign currency[61].

In 2013, networks of major South Korean banks and broadcasters were the victim of attacks traced to North Korea. The 20 March intrusions that targeted six South Korean banks and broadcasters affected 32,000 computers and disrupted banking services.

A major attack on Sony Pictures brought the movie studio to its knees in closing months of 2014. At the time, Sony was about to release *The Interview*, a comedy about a plot to kill North Korean leader Kim Jong-Un. The hackers obtained some 100 terabytes of data stolen from Sony servers (hat's roughly 10 times the entire printed collection of the Library of Congress). The data breach outed business transactions including movie scripts (for instance the James Bond series script *Spectre*), five entire films, internal memos and personal information on movie stars and Sony employees. Then they wiped computer software. Clues pointed to Lazarus, and the FBI went on to conclude that North Korea was behind the breach[62].

In September 2016 North Korean hackers stole a large cache of military documents from South Korea, including a plan to assassinate North Korea's leader Kim Jong-un. Some 235 gigabytes of military documents had been

---

[58] C. Campbell, 'The World Can Expect More Cybercrime From North Korea Now That China Has Banned Its Coal', Time online edition, 20 February 2017, available at: http://time.com/4676204/north-korea-cyber-crime-hacking-china-coal/ (accessed 8 July 2018).

[59] R. Fordoński, T*he Right to Deter and the UN Security Council Resolutions concerning North Korea Missile Program* (Olsztyn: Warmia and Mazury Universoty Press, 2018), p. 15 (quoting a statement of UN Secretary-General Ban Ki-moon following the adoption of Security Council resolution 2321 (2016) on 30 November 2016). See also SC Res 2123 (2016) of 30 November 2016; SC Res 2375(2017) of 11 September 2017; SC Res 2397 (2017) of 22 December 2017.

[60] Campbell, 'The World Can Expect More Cybercrime From North Korea', *supra* note 58. See also Fordoński, T*he Right to Deter*, *supra* note 59, p. 162.

[61] C. Kim, 'North Korea hacking increasingly focused on making money more than espionage: South Korea study', Reuters online edition, 28 July 2017, available at: https://www.reuters.com/article/us-northkorea-cybercrime/north-korea-hacking-increasingly-focused-on-making-money-more-than-espionage-south-korea-study-idUSKBN1AD0BO (accessed 8 July 2018).

[62] C. Riley and J. Mullen, 'North Korea's long history of hacking', CNN online edition, 16 May 2017, available at: http://money.cnn.com/2017/05/16/technology/ransomware-north-korea-hacking-history/index.html?iid=EL (accessed 9 July 2018); H. Wee, 'Inside North Korea's scrappy, masterful cyberstrategy', CNBC News online edition, 18 December 2014, available at: http://www.cnbc.com/2014/12/18/inside-north-koreas-scrappy-masterful-cyber-strategy.html (accessed 11 July 2018).

stolen from the Defence Integrated Data Centre, including wartime contingency plans drawn up by the US and South Korea and reports to the allies' senior commanders. Plans for the South's special forces were also reportedly accessed, along with information on significant power plants and military facilities in the South[63].

North Korea's targets have been shifting in recent years, however, and increasingly targeting financial institutions worldwide. The so called *Lazarus* group targeted and then executed the fraudulent transfer of $81 million from Bangladesh Bank, the central bank of Bangladesh, in February 2016, the largest successful cyber-theft from a financial institution to date, and engaged in computer intrusions and cyber-heists at many more financial services victims in the United States, and in other countries in Europe, Asia, Africa, North America, and South America in 2015, 2016, 2017, and 2018, with attempted losses well over $1 billion.[64] For instance, a malicious cyber campaign targeted the Polish banking sector and affected multiple victims, including Polish financial institutions between 5 October 2016 and 2 February 2017. The series of intrusions has been characterized as one of the most serious information security incidents, if not the most serious information security incident, that has occurred in Poland, nevertheless the intrusion was likely discovered before the hackers could successfully steal any funds[65].

Between 2013 and 2015, Pyongyang South Korean bitcoin exchanges, stealing approximately 100-million won (nearly US$90,000) in Bitcoin every month.[66] The *WannaCry* virus also falls in the category of revenue generation as it demanded victims pay a ransom in bitcoin, yielding more than $140,000.[67]

---

[63] 'North Korea 'hackers steal US-South Korea war plans", BBC News online edition, 10 October 2017, available at: https://www.bbc.co.uk/news/world-asia-41565281 (accessed 2 August 2018).

[64] *US v. Park Jin Hyok*, *supra* note 4, para. 8.

[65] Ibid., para. 189. Hackers behind the computer intrusions spread malware by infecting the website of the Polish Financial Supervision Authority, www.knf.gov.pl, with malware and used the compromised website in what is known as a "watering hole" attack. A watering hole attack occurs when a hacker compromises a website that is known to be visited by intended victims. As the intended victims visit the website, typically as part of their normal business practices, the intended victims (and sometimes unintended victims) are infected with malware that gives the hacker access to the intended victim networks. In this case, the subjects likely assumed numerous banks would regularly visit the website of the Polish Financial Supervision Authority, making that website an ideal candidate to be used as a watering hole to infect banks in Poland. *Ibid*., para. 190.

[66] 'Bitcoin Becomes Part Of North Korea's Geopolitical Arsenal', Oil Price, 30 September 2017, available at: https://oilprice.com/Geopolitics/International/Bitcoin-Becomes-Part-Of-North-Koreas-Geopolitical-Arsenal.html (accessed 8 July 2018).

[67] S. Pham, 'North Korea is trying to amass a bitcoin war chest', CNN online edition, 12 September 2017, available at: http://money.cnn.com/2017/09/12/technology/north-korea-hackers-bitcoin/index.html?iid=EL (accessed 9 July 2018).

Accordingly, the May 2017 ransomware did not constitute act of political coercion in the terms of illegal intervention in internal affairs of States.

2.2. *WannaCry* as illegal usurpation of a government function

The other possibility is that the *WannaCry* cyber hacking was illegal, not because it constituted a coercive intervention but rather an illegal "usurpation of an inherently governmental function",[68] which does not require the element of coercion[69].

Although the cyberattack targeted private corporations for revenue generation, government systems were also affected by the operation, which could be considered as interference with "inherently governmental functions".

The state-owned oil company Petrobras and Brazil's Foreign Ministry, the Russian Interior Ministry, and state rail monopoly Russian Railways all reported infections, as they run on the outdated Windows XP operating system. A spokesman for Russian Post, a state-owned monopoly, said no computers were infected, but some terminals were temporarily switched off as a precaution. "The virus attack did not touch Russian Post, all systems are working and stable," he claimed[70].

Disabling government computer systems "would be a violation of sovereignty, and consequently an internationally wrongful act", according to the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn.[71] The confirmation of illegal non-intervention in remains a open question, though.

First, the *WannaCry* ransomware did not target the mentioned States or their government apparatus specifically, as it was a money-making scheme that got out of control. In other words, the May 2017 attack was indiscriminate rather than targeted and those behind the attack may not have expected it to have spread as fast as it did[72].

Second, the government networks outages also illustrate what investigators said was a common misconception about *Wannacry* – infected computers were more likely to be part of antiquated systems not deemed important enough to update with the latest security patches, rather than machines integral to the company's core business.[73] Put succinctly, even if the attack

---

[68] *Tallinn Manual 2.0*, *supra* note 30, p. 24.

[69] J. D. Ohlin, 'Did Russian Cyber Interference in the 2016 Election Violate International Law?', (2017) 95 Texas L Rev (Texas Law Review) 1579–1598, 1593.

[70] J. Stubbs, 'Wannacry hits Russian postal service, exposes wider security shortcomings', Reuters online edition, 24 May 2017, available at: https://www.reuters.com/article/us-cyber-attack-russia-idUSKBN18K26O?rpc=401%26 (accessed 23 September 2018).

[71] NATO, 'WannaCry Campaign', *supra* note 26.

[72] Corera, 'NHS cyber-attack was ‚launched from North Korea", *supra* note 10.

[73] Stubbs, 'Wannacry hits Russian postal service', *supra* note 70.

caused huge disruption in the short term, it did not affect vital computer systems.

Subsequently, no illegal usurpation of a government function could be confirmed as the result of the May 2017 ransomware cyberattack.

Summing up, there are two conditions precedent to finding a violation of the prohibition of non-intervention in internal affairs of other States. First, the prohibition only applies to matters that fall within another State's *domaine réservé*. Second, to qualify as prohibited intervention, the act in question must involve coercion. As observed above, none of the conditions are fulfilled in the discussed case.

In effect, the principle of non-intervention was not violated by the alleged North Korean cyberintrusions on 12 May 2017.

3. *WannaCry* as use of force

Article 2(4) of the UN Charter prohibits what could be described as a "particularly obvious example" of intervention:[74] "All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state."[75]

Article 2(4) does not expressly define the term "force". One commentator observes, however: "U.N. Charter makes clear that at either end of the spectrum, it is apparent what is force and what is not force. On one end, traditional military force using conventional military weapons clearly constitutes a use of force. On the other end, political or economic coercion does not constitute a use of force, as the purpose of the United Nations and the U.N. Charter "is to maintain international peace and security" and "to save succeeding generations from the scourge of war." By excluding economic and political coercion from the definition of force, the drafters indicated that uses of force in violation of Article 2(4) focus strictly on military instruments. The boundary between a use of force and a non-use of force therefore lies within the area between an exercise of traditional military coercion and an exercise of political or economic coercion."[76]

Two acclaimed academics disagree, specifically in the context of the *WannaCry* cyberattack: "Whether non-destructive and non-injurious cyber operations can qualify as uses of force is unsettled. In the absence of State practice and *opinio juris*, it is difficult to determine if and when States will treat them as such. (...) Nevertheless, in our view, hostile cyber operations of

[74] *Nicaragua* case (Merits), *supra* note 52, para. 205.

[75] UN Charter, *supra* note 39, Art. 2(4).

[76] R. Nguyen, 'Navigating Jus Ad Bellum in the Age of Cyber Warfare', (2013) 101(4) California LR (California Law Review) 1079–1130, 1113–1114.

a significant scope and scale that disrupt the provision of healthcare could reasonably be viewed as a use of force. By contrast, we believe it unlikely that States will treat non-destructive cyber operations directed against or affecting private firms as uses of force absent at least a major disruption of the national economy."[77]

To identify legal character of the *WannaCry* ransomware attack under prohibition of use of force in international relations the following analysis will use three analytical approaches, developed in doctrine in reference to definition of use of force:

(1) an instrument-based approach,
(2) a target-based approach, and
(3) an effects-based approach[78].

3.1. *WannaCry* and the instrument-based definition of use of force

The instrument-based definition of the term "use of force" looks at the mode of attack and whether the weapon used possesses "physical characteristics traditionally associated with military coercion." Thus, "[t]he more analogous a new weapon is to conventional forms of military force, the more likely its operation will constitute a 'use of force' or 'armed attack.'"[79]

This approach is derived from a textualist reading of the UN Charter. The Charter "uses the terms 'use force',[80] 'armed force',[81] and 'armed forces'[82] interchangeably",[83] specifying that "armed force is action by air, sea, or land forces", which includes "demonstrations, blockade, and other operations by air, sea, or land forces"[84] but does not include "complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communication, and the severance of diplomatic relations."[85]

Under this reading, it would appear the Charter's drafters understood that force meant traditional military armed force and excluded other forms of coercion[86]. This view is strengthened by the UN General Assembly resolution on the definition of aggression, which includes armed invasions, port blocka-

---

[77] Schmitt and Fahey, 'WannaCry and the International Law of Cyberspace', *supra* note 4.
[78] R. Patterson, 'Silencing the Call to Arms: A Shift Away From Cyber Attacks as Warfare', (2015) 48 Loyola L A L Rev (Loyola of Los Angeles Law Review) 969–1016, 988.
[79] Nguyen, 'Navigating Jus Ad Bellum in the Age of Cyber Warfare', *supra* note 76, 1117.
[80] UN Charter, *supra* note 39, Art. 2(4).
[81] Ibid., Preamble; Art. 41.
[82] Ibid., Arts. 43–44; 46–47.
[83] Nguyen, 'Navigating Jus Ad Bellum in the Age of Cyber Warfare', *supra* note 76, 1118.
[84] UN Charter, *supra* note 39, Art. 42.
[85] Ibid., Art. 43.
[86] Patterson, 'Silencing the Call to Arms', *supra* note 78, 989.

des, bombardments, and armed violations of territory[87]. Each of these examples involves physical force and violations of territoriality. By this definition then, cyber attacks are not capable of rising to the levels of uses of force because computer code is neither a physical nor a conventional military force[88].

As even cyberattacks that result in tangible physical destruction would be outside the purview of the *jus ad bellum* under this approach, the *WannaCry* ransomware could not be identified as the case of use of force.

3.2. *WannaCry* and the target-based definition of use of force

The target-based approach takes the opposite tack: it looks at the object of attack, and "automatically treats *any* cyber attack against critical ... infrastructure as an armed attack because of the potential for severe consequences if such [infrastructure were] disabled."[89]

Under this approach, emphasis is put on the status of the target, with "critical infrastructure" given privileged significance. If an cyberattack is made on critical infrastructure, it constitutes automatically use of force, regardless of whether it comports with traditional military force[90].

The target-based definition of use of force is supported by States represented in the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security[91]. They agreed in 2015 that "[a] State should not conduct or knowingly support [information and communications technology] activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public".[92]

The problem with the target-based approach, however, is that each State individually defines what constitutes its critical infrastructure. The United States, for instance, designates sixteen sectors as critical infrastructure, including "food and agriculture, banking and finance, commercial facilities, communications, healthcare, and transportation" facilities[93].

---

[87] GA Res 3314(XXIX) of 14 December 1974, Definition of Aggression, Annex, Art. 3.

[88] Patterson, 'Silencing the Call to Arms', *supra* note 78, 989.

[89] Nguyen, 'Navigating Jus Ad Bellum in the Age of Cyber Warfare', *supra* note 76, 1117, 1119.

[90] Patterson, 'Silencing the Call to Arms', *supra* note 78, 989.

[91] 20 States participating in the Group in 2015 included Belarus, Brazil, China, Colombia, Egypt, Estonia, France, Germany, Ghana, Israel, Japan, Kenya, Malaysia, Mexico, Pakistan, the Russian Federation, Spain, the United Kingdom and the United States of America. See UN Group of Governmental Experts on Developments in the Field of Information, *supra* note 45, Annex.

[92] Ibid., para. 13(f).

[93] White House, Presidential Policy Directive – Critical Infrastructure Security and Resilience, 12 February 2013, available at: https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil (accessed

According to the Directive 2013/40/EU of the European Parliament and of the Council, the term "critical infrastructure" could be understood as "an asset, system or part thereof located in Member States, which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, such as power plants, transport networks or government networks, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions."[94]

The Russian Federation identifies "vital structures": "facilities, systems and institutions of a State, deliberate influence on the information resources of which may have consequences that directly affect national security (transport, power supply, credit and finance, communications, State administrative bodies, defence system, law enforcement agencies, strategic information resources, scientific facilities and scientific and technological developments, installations entailing a high degree of technological or ecological risk, bodies for the mitigation of the effects of natural disasters or other emergencies."[95]

Note that every national list of critical infrastructure includes facilities related to health protection. The conclusion is supported by the General Assembly resolution 58/199 of 30 January 2004, defining critical infrastructures as including "those used for, *inter alia*, food distribution and public health – and the critical information infrastructures that increasingly interconnect and affect their operations."[96]

Subsequently, *WannaCry* clearly impaired the use of critical infrastructure: it severely disrupted the functioning of UK hospitals, among many other affected entities. While 80 out of 236 NHS trusts across England were affected either because they were infected or because they had to disconnect as a precaution, at least 37 NHS trusts and an additional 603 primary care or other NHS organizations were infected were in fact infected with *WannaCry*[97].

---

24 September 2018) ("The term "critical infrastructure" has the meaning provided in section 1016(e) of the USA Patriot Act of 2001 (...), namely systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.").

[94] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, OJ L 218, 14 August 2013, Preamble, para. 4.

[95] Developments in the field of information and telecommunications in the context of international security, Report of the Secretary-General, UN Doc A/55/140, 10 July 2000, available at: http://undocs.org/A/55/140 (accessed 18 August 2018), 4.

[96] GA Res 58/199, Creation of a global culture of cybersecurity and the protection of critical information infrastructures, 30 January 2004, Preamble.

[97] *US v. Park Jin Hyok*, *supra* note 4, para. 225.

The ransomware did not, however, target the UK or the NHS specifically. As the UK Prime Minister Theresa May stated on 15 May 2017, "It was clear warnings were given to hospital trusts, but this is not something that focused on attacking the NHS here in the UK."[98] Rather, disruptions caused by the ransomware were unintended collateral damage of the money-making scheme, exposed to accidental intrusion due to the fact that 90% of UK hospitals still had machines running on Windows XP[99].

Problematic is also scale of the cyberattack. First, more than 80% of the NHS computer network was unaffected by the ransomware.[100] Second, even as the attack held hospitals hostage by freezing computers, encrypting data and demanding money through online bitcoin payments, it appeared still to be "low-level" stuff. Ori Eisen, who founded the Trusona cybersecurity firm in Arizona, said on 13 May 2017, said the same thing could be done to crucial infrastructure, like nuclear power plants, dams or railway systems: "This is child's play, what happened. This is not the serious stuff yet. What if the same thing happened to 10 nuclear power plants, and they would shut down all the electricity to the grid? What if the same exact thing happened to a water dam or to a bridge? Today, it happened to 10,000 computers. There's no barrier to do it tomorrow to 100 million computers."

In other words, the attack's impact was said to be relatively low compared to other potential attacks of the same type if it had been specifically targeted on highly critical infrastructure, like nuclear power plants, dams or railway systems.[101]

Last but not least, Health Secretary Jeremy Hunt described *WannaCry* as "criminal activity".[102] Therefore, he excluded explicitly the possibility of qualification of the malware in the terms of the target-based use of force.

3.3. *WannaCry* and the effects-based definition of use of force

Finally, the effects-based approach analyzes the consequences of an attack to determine whether it rises to the level of a use of force or armed attack.[103] The first edition of the *Tallinn Manual* uses the "scale and effects" test. According to a commentary to Rule 11 of the *Tallinn Manual 1.0*, "The Experts found the focus on scale and effects to be an equally useful approach

---

[98] 'No ,second spike' but disruption continues', *supra* note 5.

[99] Cellan-Jones, 'Ransomware and the NHS – the inquest begins', *supra* note 2.

[100] 'No ,second spike' but disruption continues', *supra* note 5 (quoting UK Health Secretary Jeremy Hunt).

[101] 'Global 'WannaCry' ransomware cyberattack seeks cash for data', *supra* note 3.

[102] 'No ,second spike' but disruption continues', *supra* note 5.

[103] Patterson, 'Silencing the Call to Arms', *supra* note 78, 991.

when distinguishing acts that qualify as uses of force from those that do not. In other words, 'scale and effects' is a shorthand term that captures the quantitative and qualitative factors to be analysed in determining whether a cyber operation qualifies as a use of force."[104]

Accordingly, a cyber attack that produces physical destruction similar to that produced by a kinetic attack is more likely to qualify as a use of force, while one that produces political or economic coercion will not[105]. Acts that injure or kill persons or damage or destroy objects are unambiguously uses of force[106]. The *Tallinn Manual 2.0* concludes that certain operations not generating such consequences may also cross the use of force threshold. Agreement on a bright line test for qualification of non-destructive or non-injurious cyber operations as a use of force proved elusive. This being so, the experts proposed an approach that assesses the likelihood of States characterizing a cyber operation as such. It is based "on the premise that in the absence of a conclusive definitional threshold, States contemplating cyber operations, or that are the target thereof, must be highly sensitive to the international community's probable assessment of whether the operations violate the prohibition of the use of force."[107]

The method highlights factors that States are likely to focus on when making use of force determinations. Key ones include: severity of consequences; immediacy of consequences; directness of consequences; invasiveness of the operation; measurability of consequences; military character of the operation; extent of State involvement; and any presumptive legality on the type of operation, as in the case of psychological operations or espionage[108]. Other factors that the experts identified as relevant include: "the prevailing political environment, whether the cyber operation portends the future use of military force, the identity of the examiner, any record of cyber operations by the attacker, and the nature of the target."[109]

With the exception of severity, no single factor alone is likely to qualify a cyber operation as a use of force. Instead, these and other factors are considered together when assessing the likelihood that the operation in question will qualify as a use of force[110].

Applying the abovementioned requirements to the *WannaCry* case, it should be noted that the estimated damage it caused could exceed $1 billion,

---

[104] *Tallinn Manual on the International Law Applicable to Cyber Warfare: Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence* (Cambridge: Cambridge University Press, 2013), pp. 45–46.

[105] Nguyen, 'Navigating Jus Ad Bellum in the Age of Cyber Warfare', *supra* note 76, 1122.

[106] *Tallinn Manual 1.0*, *supra* note 104, p. 48.

[107] *Tallinn Manual 2.0*, *supra* note 30, p. 333.

[108] Ibid., pp. 333–336.

[109] Ibid., p. 336.

[110] Schmitt, 'Grey Zones in the International Law of Cyberspace', *supra* note 27, 14–15.

according to the report, despite only around $100,000 in bitcoins paid in ransoms to the perpetrators.[111] Multiple lives was also put in immediate danger or even lost in the result of the cyberattack on the NHS. *Prima facie*, there was no patient harm reported during the incident[112]. Some observers claimed, however, that as the effects included 6,912 appointments that were cancelled (and subsequently re-scheduled) between 12 and 18 May 2017, and 1,220 (approximately 1%) pieces of diagnostic equipment across the NHS that were affected by *WannaCry*,[113] "[p]atients in the UK lost valuable medical response time (and it is very likely that one could honestly say *WannaCry* ended up causing mortal harm to some)."[114] Subsequently, *WannaCry* ended up causing undetermined number of deaths in addition to "hundreds of millions of dollars in damages to medical production lines and other business processes."[115]

Does it mean that *WannaCry*, although in unintended way, constituted a use of force?

A cyber operation, like any operation, resulting in damage, destruction, injury, or death is highly likely to be considered a use of force. That generating mere inconvenience or irritation will never do so.[116] The *WannaCry* ransomware attack could be described in both ways. The immediacy and directness factors – focusing on the temporal aspect and the chain of causation, respectively, of the consequences in question[117] – play, however, on favour of the non-use of force characterization. The *Tallinn Manual 1.0* claims that "States harbour a greater concern about immediate consequences than those that are delayed or build slowly over time, and are more likely to characterize a cyber operation that produces immediate results as a use of force than cyber actions that take weeks or months to achieve their intended effects."[118]

WannaCry-related deaths, if actually occured, took place mostly weeks and months after the cyberattack as thousands appointments, including operations were cancelled – including at least 139 people potentially with cancer, who had urgent referrals cancelled – and computers in over 600 doc-

---

[111] A. Cuthbertson, 'Ransomware Attacks Rise 250 Percent in 2017, Hitting U.S. Hardest', Newsweek online edition, 23 May 2017, available at: http://www.newsweek.com/ransomware-attacks-rise-250-2017-us-wannacry-614034 (accessed 6 July 2018).

[112] *US v. Park Jin Hyok*, *supra* note 4, para. 225.

[113] Ibid.

[114] J. Crowe, 'What Makes SamSam, the Ransomware that Crippled Atlanta, So Different', Barkly, 8 May 2018, available at: https://blog.barkly.com/what-is-samsam-ransomware-2018 (accessed 21 September 2018).

[115] Ibid. (quoting Bob Rudis, chief security data scientist at Rapid7).

[116] *Tallinn Manual 1.0*, *supra* note 104, p. 48.

[117] Ibid., p. 49.

[118] Ibid., p. 49.

tor's surgeries infected[119]. More immediate deaths are also possible but it is not known how many ambulances and individuals were diverted from five accident and emergency departments unable to treat some patients[120]. In armed actions, by contrast, "cause and effect are closely related. An explosion, for example, directly harms people or objects. Cyber operations in which the cause and effect are clearly linked are more likely to be characterized as uses of force."[121]

Going further, requirement of invasiveness refers to the degree to which cyber operations intrude into the target State or its cyber systems contrary to the interests of that State. As a rule, the more secure a targeted cyber system, the greater the concern as to its penetration. Intrusion into a military system is more invasive than merely exploiting vulnerabilities of an openly accessible system in a hospital or small business.[122] Accordingly, a nexus between the cyber operation in question and military operations heightens the likelihood of characterization as a use of force.[123] *WannaCry* was a isolated case of ransomware not connected to any known action of North Korea'a armed forces, like a missile or nuclear test.

Therefore, it is concluded that *WannaCry* did not constitute a use of force prohibited under Article 2(4) of the UN Charter despite the fact that it caused a considerable damage on a global scale and possible deaths in the UK albeit in an unintended way.

Conclusions

In May 2017 *WannaCry* infected more than 300,000 machines in 150 countries, causing billions of dollars in damages and grinding global business to a halt. The speed and scale of the attack was obviously notable, but it's *WannaCry*'s legacy that resonates today. The cyberlandscape has fundamentally changed, with threat actors increasing almost exponentially in their capabilities, sophistication and ambition. "*WannaCry* changed the cybersecurity game, not just through its outsized impact; it made waves because of its outsized influence on the cyber-threat landscape", Check Point researchers said in a blog breaking down the implications. "Marking a turn-

[119] 'North Korea calls UK WannaCry accusations 'wicked", BBC News online edition, 31 October 2017, available at: https://www.bbc.co.uk/news/world-asia-41816958 (accessed 2 August 2018); 'NHS 'could have prevented' WannaCry ransomware attack', BBC News online edition, 27 October 2017, available at: https://www.bbc.co.uk/news/technology-41753022 (accessed 2 August 2018).

[120] Ibid.

[121] *Tallinn Manual 1.0*, *supra* note 104, p. 49.

[122] Ibid.

[123] Ibid., p. 50.

ing point in the cybersecurity environment, we were looking at the first global-scaled, multi-vectored cyberattack powered by state-sponsored tools. WannaCry marked a new generation of cyberattacks."[124]

The stakes are higher than ever before as well. *WannaCry* demonstrated that cyberattacks can introduce real, physical risks into the equation. According to Rishi Bhargava, co-founder at Demisto, "*WannaCry* was unique because this was the first large ransomware attack targeted at the healthcare vertical and affected not only computers, but also many medical devices like MRI machines."[125]

The last feature of the *WannaCry* – "putting the lives of people at risk"[126] – is a starting point of its legal analysis under contemporary international law. Assuming that the ransomware attack was attributable to North Korea, a topic discussed also above, the question is whether the operation breached any international law obligations North Korea owed another State, such that it constituted an "internationally wrongful act." In cases involving States, the international law rules most likely to be violated are the prohibition on the use of force, the prohibition on intervention into other States' internal or external affairs and the obligation to respect the sovereignty of other States.

There is general agreement that destructive operations or those that are injurious cross the use of force threshold, and thus constitute a violation of Article 2(4) of the UN Charter and customary international law; the *WannaCry* operation did not appear to reach this level. Whether non-destructive and non-injurious cyber operations can qualify as uses of force is unsettled. In the absence of State practice and *opinio juris*, it is difficult to determine if and when States will treat them as such. The experts participating in the Tallinn Manuals project, suggest factors that States are likely to consider when making these assessments, but were unable to articulate any bright line test. Nevertheless, hostile cyber operations of a significant scope and scale that disrupt the provision of healthcare – in contrast to non-destructive cyber operations directed against or affecting private firms, absent at least a major disruption of the national economy – could reasonably be viewed as a use of force.

---

[124] T. Seals, 'One Year After WannaCry: A Fundamentally Changed Threat Landscape', Threatpost, 17 May 2018, available at: https://threatpost.com/one-year-after-wannacry-a-fundamentally-changed-threat-landscape/132047/, (accessed 25 September 2018).

[125] Crowe, 'What Makes SamSam, the Ransomware that Crippled Atlanta, So Different', *supra* note 114.

[126] Seals, 'One Year After WannaCry', *supra* note 124 (quoting Brian NeSmith, CEO and co-founder at Arctic Wolf Networks as stating: "For industries like healthcare, ransomware puts the lives of people at risk. (...) Today, the focus is on PCs, but tomorrow, everything from machinery, power control systems, industrial sensors and even thermostats will be targets. In the case of machinery, it could impact the safety and well-being of workers, dramatically increasing the stakes beyond just the ransom money.").

The *WannaCry* cyberattack raises a further question of law. The extent to which the attacks were directed at particular entities is unclear and NHS England "was not the specific target" of the operation. But, assuming for the sake of discussion that the attacks were indiscriminate, could they nevertheless qualify as uses of force vis-à-vis States that might have suffered qualifying consequences? Schmitt and Fahey state they could, "so long as the nature of the consequences was foreseeable, even if the attacker may not have known precisely where they would manifest."[127] That this issue remains, however, unresolved under international law and the Authors promote a opposing view, underlying that *WannaCry* was a money-making scheme that got out of control as those behind the attack may not have expected it to have spread as fast as it did.

The same is not true with respect to the prohibition on intervention into other States' internal or external affairs. Intervention has two elements. First, the act must relate to the target State's *domaine réservé* (field of activity that is not committed to international law regulation). Certain *WannaCry* attacks did so, particularly those affecting law enforcement. For instance, over 1,000 computers of the Russian Interior Ministry were compromised, as was 25 percent of India's Andhra Pradesh police department network.

However, the operation arguably did not satisfy the second criterion, that the act be coercive. A coercive cyber operation is one that causes a State to engage in conduct in which it would otherwise not engage, or refrain from conduct in which it would otherwise engage. *WannaCry* was disruptive, but not coercive in this sense.

The *WannaCry* cyberattack might, however, be considered a violation of the sovereignty of certain affected States. The *Tallinn Manual 2.0* experts concur that a violation occurs whenever a cyber operation either causes damage to cyber infrastructure in another State or interferes with an inherently governmental act, the paradigmatic example being the conduct of elections. Most of them also agreed that "damage" includes a permanent loss of functionality or one that requires physical repair of the damaged infrastructure, such as replacement of the hard drive.

That does not appear to have occurred this time. Nevertheless, the operation did in some respects violate the sovereignty of a number of States, particularly in light of the significant disruption of functions, which the *Tallinn Manual 2.0* would count as "damage", necessary for the delivery of medical care.

Moreover, the operation interfered with an inherently governmental function – law enforcement.[128]

---

[127] Schmitt and Fahey, 'WannaCry and the International Law of Cyberspace', *supra* note 4.
[128] See also ibid.

Summing up the analysis, hackers behind the *WannaCry* ransomware attack clearly committed a wide range of criminal offences under national law of the affected States. In the UK, this is likely to include a breach of the newly introduced section 3ZA of the Computer Misuse Act 1990 which carries a life sentence.[129] The cyberattack was also a violation of international law. As some questions remain open, pending a clear States determination and public explanation how international law applies to attacks like *WannaCry*, it is safe to assume that the violation did not involve use of force in international relations or illegal intervention in internal affairs of affected States.

Literature

Dickinson E., *The equality of states in international law* (Cambridge: Harvard University Press, 1920).

Fordoński R., T*he Right to Deter and the UN Security Council Resolutions concerning North Korea Missile Program* (Olsztyn: Warmia and Mazury Universoty Press, 2018).

Jennings R., Watts A., *Oppenheim's International Law* (London/New York: Longman, 2008).

Kilovaty I., *Doxfare: Politically Motivated Leaks and the Future of the Norm on Non-Intervention in the Era of Weaponized Information*, (2018) 9 Harvard NSJ (Harvard National Security Journal) 146–179.

Nguyen R., *Navigating Jus Ad Bellum in the Age of Cyber Warfare*, (2013) 101(4) California LR (California Law Review) 1079–1130.

Ohlin J.D., *Did Russian Cyber Interference in the 2016 Election Violate International Law?*, (2017) 95 Texas L Rev (Texas Law Review) 1579–1598.

Patterson R., *Silencing the Call to Arms: A Shift Away From Cyber Attacks as Warfare*, (2015) 48 Loyola L A L Rev (Loyola of Los Angeles Law Review) 969–1016.

Schmitt M.N., Watts S., *Beyond State-Centrism: International Law and Non-state Actors in Cyberspace*, (2016) 21(3) JCSL (Journal of Conflict & Security Law) 595–611.

Schmitt M.N., *Grey Zones in the International Law of Cyberspace*, (2017) 42(2) Yale JIL (Yale Journal of International Law) 1–21.

Schmitt M.N., *Peacetime Cyber Responses and Wartime Cyber Operations Under International Law: An Analytical Vade Mecum*, (2017) 8 Harvard NSJ (Harvard National Security Journal) 239–282.

Schmitt M.N., *'Virtual' Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law*, (2018) 19(1) Chicago JIL (Chicago Journal of International Law) 30–67.

Tallinn Manual on the International Law Applicable to Cyber Warfare: Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence (Cambridge: Cambridge University Press, 2013).

[129] *R. Cumbley, V. Havard-Williams and T. Cassels,* 'UK – Reflections on the WannaCry cyber attack', Linklaters, July 2017, available at: https://www.linklaters.com/pl-pl/insights/publications/tmt-news/tmt-news---june-2017/uk---reflections-on-the-wannacry-cyber-attack (accessed 9 July 2018).

Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations Prepared by the International Groups of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence (Cambridge/New York: Cambridge University Press, 2017).

Streszczenie

Atak z użyciem oprogramowania szantażującego *WannaCry* jako naruszenie prawa międzynarodowego

Słowa kluczowe: wirus *WannaCry*, oprogramowanie szantażujące, grupa *Lazarus*, pojęcie i zakres suwerenności państw w cyberprzestrzeni, zakaz interwencji w sprawy wewnętrzne państw, zakaz użycia siły w relacjach międzynarodowych.

Artykuł podejmuje temat cyberataku, dokonanego 12 maja 2017 r. przy użyciu wirusa oprogramowania szantażującego w postaci złośliwego wirusa *WannaCry*. Największy tego typu atak w historii objął do 300 tysięcy komputerów w ponad 150 krajach, powodując straty w wysokości przekraczającej jeden miliard dolarów USA. Podczas gdy zainfekowany komputer wyświetlał informację o zaszyfrowaniu zawartości dysku, odzyskanie danych było możliwe (ale nie gwarantowane) po wpłaceniu „okupu", czyli określonej sumy pieniędzy, płatnej w Bitcoinach. W wyniku ataku ucierpiały zarówno tysiące podmiotów prywatnych, jak i sieci rządowe oraz przedsiębiorstwa państwowe. Wśród tych ostatnich do szczególnie poszkodowanych należały brytyjska publiczna służba zdrowia, rosyjskie Ministerstwo Spraw Wewnętrznych oraz sieci rządowe w Brazylii.

W grudniu 2017 r. sześć państw, w tym Stany Zjednoczone i Zjednoczone Królestwo Wielkiej Brytanii, oficjalnie przypisało cyberatak z maja tr. Koreańskiej Republice Ludowo-Demokratycznej. Przypisanie odpowiedzialności nie było jednak równoznaczne z potwierdzeniem faktu naruszenia prawa międzynarodowego oraz wskazaniem jego zakresu. Poniższa analiza dokonuje takiej oceny z perspektywy wybranych zasad Karty Narodów Zjednoczonych: zasady suwerenności państw w cyberprzestrzeni, zakazu interwencji w sprawy wewnętrzne państw oraz zakazu użycia siły w relacjach międzynarodowych.