2019 11th International Conference on Cyber Conflict:
Silent Battle
T. Minárik, S. Alatalu, S. Biondi,
M. Signoretti, I. Tolga, G. Visky (Eds.)
2019 © NATO CCD COE Publications, Tallinn

Permission to make digital or hard copies of this publication for internal use within NATO and for personal or educational use when for non-profit or non-commercial purposes is granted providing that copies bear this notice and a full citation on the first page. Any other reproduction or transmission requires prior written permission by NATO CCD COE.

SamSam and the Silent Battle of Atlanta

Kenneth Kraszewski
LLD Candidate
Faculty of Law
University of Helsinki
Helsinki, Finland
kenneth.kraszewski@helsinki.fi

Abstract: The SamSam ransomware attack on Atlanta in early 2018 crippled municipal services in a major American city without the firing of a single shot, epitomizing the notion of a "Silent Battle". Atlanta was not the only battlefield. Municipal governments in Colorado and New Mexico, as well as medical associations in Indiana, Virginia, New York and Buffalo, were all targets. While other ransomware or ransomware-like attacks have been larger-scale events, the SamSam ransomware attacks deserve an international law analysis.

This article examines the SamSam attacks on health care providers and municipal government through the lens of the second Tallinn Manual. First, it explains the SamSam ransomware itself and Gold Lowell, the group presumed to be behind it. Second, this article explores how the SamSam incidents might be classified under international law. This article asks whether ransomware attacks are internationally wrongful acts – breaches of international obligations attributable to a State. This entails considering whether a ransomware attack may be legally classified as a use of force, an intervention, a violation of sovereignty, or a breach of an international law obligation. Finally, this article discusses the possible legal responses to the SamSam ransomware attacks available to the United States: countermeasures, the plea of necessity, acts of self-defense under Article 51 of the U.N. Charter, and acts of retorsion.

Keywords: *attribution, cyber attack, due diligence, non-intervention, ransomware, sovereignty*

1. INTRODUCTION

In March 2018, the municipal government of Atlanta was "brought to its knees" by a ransomware attack deemed "one of the most sustained and consequential cyberattacks ever mounted against a major American city".[1] The city's court – "the busiest court" in the South-eastern United States[2] — was unable to validate warrants, policer officers were forced to issue citations by hand, and the city's employment application portal was shut down.[3] Years of digital files were rendered inaccessible.[4] The attack was costly. Its perpetrators demanded $51,000 to restore Atlanta's systems to full functionality, but the city followed the advice of federal authorities and refused payment. One month later, Atlanta had spent over $2.6 million to restore its systems;[5] an additional $9.5 million was later requested.[6] Atlanta is not alone in its misery. The same hacking group and malware have been implicated in attacks on hospital and health services providers and municipal governments across the United States.

In 2016, hospital systems in Baltimore were infected.[7] The following year, Buffalo's primary trauma center was hit. With computers offline, staff resorted to paper charts, transmitted messages in person, and viewed X-rays on traditional light boxes.[8] Clinics and doctors' offices in Virginia lost access to patient files when the systems of an electronic health records company were infected in early 2018.[9] A hospital in Greenfield, Indiana was infected simultaneously, leaving 1,400 files, including patient medical records, inaccessible.[10]

While Atlanta received more attention, other municipal governments were also victims. Two thousand computers at the Colorado Department of Transportation were encrypted in late February 2018. Colorado spent up to $1.5 million to remediate the

1 Alan Binder & Nicole Perlroth, *A Cyberattack Hobbles Atlanta, and Security Experts Shudder*, N.Y. TIMES, Mar. 27, 2018, https://nyti.ms/2Gf7oRX.

2 Rhonda Cook, *Court Hit by Hack Struggles to Recover*, ATLANTA J.-CONST., June 10, 2018, at B1, 2018 WLNR 17814216.

3 Binder & Perlroth, *supra* note 1.

4 Charles Bethea, *The Seemingly Random and Definitely Worrisome Cyberattack on Atlanta*, THE NEW YORKER, Mar. 29, 2018, https://perma.cc/E982-5NL3.

5 Lily Hay Newman, *Atlanta Spent $2.6M to Recover From $52,000 Ransomware Scam*, WIRED, Apr. 23, 2018, https://perma.cc/3CBJ-PF2M.

6 *Atlanta Officials Reveal Worsening Effects of Cyber Attack*, 6/6/18 Reuters News 22:50:01, June 6, 2018.

7 Ian Duncan et al., *MedStar Hackers Demand Ransom*, BALT. SUN, Mar. 31, 2016, at 1, 2016 WLNR 9768566.

8 Henry L. Davis, *How ECMC Got Hacked by Cyber Extortionists*, BUFF. NEWS, May 20, 2017, 2017 WLNR 15750503.

9 Cathy Dyson, *Fredericksburg Clinic, Doctors' Offices Crippled by Virus—the Computerized Kind*, FREE LANCE-STAR (Fredericksburg, Va.), Jan. 22, 2018, 2018 WLNR 2228939.

10 Vic Ryckaert, *Hospital Pays $50K Ransom for Patient Data*, INDIANAPOLIS STAR (Indianapolis, Ind.), Jan. 18, 2018, A01, 2018 WLNR 1767864.

effects.[11] SamSam ransomware shut down systems in Farmington, New Mexico, disrupting bill paying and record processing services.[12]

The WannaCry, Petya and NotPetya ransomware incidents of 2017 have garnered greater media coverage than SamSam. WannaCry infected hundreds of thousands of systems across the world, wreaking havoc on the United Kingdom's National Health Service, the Russia Interior Ministry, and India's Andhra Pradesh police department.[13] Petya, like WannaCry, made use of code stolen from the U.S. National Security Agency and leaked online.[14] It began as an attack on Ukrainian government and business computer systems on the day before a holiday marking the adoption of Ukraine's first post-Soviet constitution.[15] Petya spread to affect systems across the globe. Soon thereafter, a variant of Petya struck in Ukraine: deemed "NotPetya", this follow-on event was determined to not be a traditional ransomware attack. Instead, researchers have concluded that the attack, which targeted the computer systems of banks, energy firms and an airport, primarily in Ukraine, was carried out by Russian government hackers. The ransomware component was a ruse designed to trick its victims into believing the attacks were being conducted by a "mysterious hacker group".[16]

While WannaCry, Petya and NotPetya were larger scale events, the SamSam ransomware also deserves an international law analysis; because its effects manifested in a single State, the analysis is perhaps more straightforward. This article considers the attacks on health care providers and municipal government through the lens of the *Tallinn Manual 2.0 on International Law Applicable to Cyber Operations ("Tallinn Manual 2.0")*.[17] The SamSam ransomware and the group behind it are explained in Part 2. Part 3. explores how the SamSam incidents might be classified under international law, and Part 4. discusses the possible responses available to the United States.

This article purposely avoids considering the ransomware campaign under the auspices of the Convention on Cybercrime of the Council of Europe ("Budapest Convention")[18] in order to consider how such attacks may be analyzed through the

11 Tamara Chuang, *After Online Derailment, CDOT Mostly on Track*, DENV. POST, Apr. 6, 2018, 14A, 2018 WLNR 10601275.

12 Hannah Grover, *City of Farmington Recovering After SamSam Ransomware Attack*, DAILY TIMES (Farmington, N.M.), Jan. 18, 2018, 2018 WLNR 1861786.

13 Michael Schmitt and Sean Fahey, *WannaCry and the International Law of Cyberspace*, JUST SECURITY, Dec. 22, 2017, https://perma.cc/QJ7W-GY7K.

14 Nicole Perlroth et al., Cyberattack Hits Ukraine Then Spreads Internationally, N.Y. Times, June 27, 2017, https://www.nytimes.com/2017/06/27/technology/ransomware-hackers.html.

15 *Id*.

16 Ellen Nakashima, *Ukraine Attack Used a Ransomware Ruse*, WASH. POST, June 30, 2017, at A12, 2017 WLNR 20082512

17 INT'L GRP. OF EXPERTS, NATO COOP. CYBER DEF. CTR. OF EXCELLENCE, TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS (Michael N. Schmitt ed., 2017) [hereinafter TALLINN MANUAL 2.0].

18 Council of Europe, Convention on Cybercrime, European Treaty Series, No. 185 (Budapest, opened for signature 23 Nov. 2001, entered into force 1 July 2004).

Tallinn Manual 2.0. While the Budapest Convention may, in certain circumstances, be a better vehicle for bringing the perpetrators of malicious cyber incidents to justice, it has significant drawbacks. It does not apply to State actors or the nationals of non-member States, and its scope differs significantly from that for the *Tallinn Manual 2.0*. The former focuses on harmonizing national laws to counter cybercrime, whereas the latter is principally concerned with whether and how international law applies to malicious activities in cyberspace. This article, in keeping with the approach of the *Tallinn Manual 2.0*, will consider whether the SamSam attacks may be characterized as internationally unlawful acts and the possible responses available to the United States, rather than considering whether they should be treated as cybercrimes under the Budapest Convention and the remedies available under that instrument.

2. GOLD LOWELL AND SAMSAM

The group behind the SamSam ransomware attacks has been named "Gold Lowell" by cybersecurity researchers.[19] Gold Lowell's members were first believed to reside in Eastern Europe,[20] but later alleged to be Iranians.[21] Security researchers presume that the group's members are not native English speakers based on "linguistic errors" in the ransom notes and transaction communications.[22] Gold Lowell is believed to have privately developed the SamSam ransomware.[23]

Unlike other forms of ransomware, SamSam is directly targeted. Attacks are focused on healthcare providers and municipal governments. SamSam is not commodity ransomware sold to other actors on online forums. The software is closely held and updated frequently to thwart antivirus detection.[24] Gold Lowell has utilized different means to gain access to servers. In 2015 and 2016, they scanned for Java vulnerabilities. Later, the group moved on to target Microsoft's IIS, file transfer protocol, and remote desktop protocol ("RDP"). As of May 2018, the group was primarily focused on accessing networks through "single-factor" external access protocols, such as RDP or virtual private networks.[25] Several tools are used once the group has gained access to the network, and Gold Lowell "is known to move from file to file, manually encrypting hundreds of systems".[26] Once encryption is complete, an apologetic message is displayed demanding payment of a certain sum in exchange for decryption.[27] The SamSam group purposely sets the price at a level

19 Secureworks, *SamSam Ransomware Campaigns*, Feb. 15, 2018, https://perma.cc/L4EP-J2W6.
20 Steve Ragan, *SamSam Explained*, CSO, Apr. 18, 2018, https://perma.cc/DP4W-YJUH
21 Nicole Perlroth & Katie Benner, *Iranians Accused in Cyberattacks*, N.Y. TIMES, Nov. 28, 2018, https://www.nytimes.com/2018/11/28/us/politics/atlanta-cyberattack-iran.html.
22 Secureworks, *supra* note 19.
23 Ragan, *supr*a note 20.
24 *Id*.
25 *Id*.
26 Nicole Perlroth, *Digital Thieves Rely on Ransom*, HOUS. CHRON., May 14, 2017, at A001, 2017 WLNR 15134229.
27 Christopher Boyd, Malwarebytes, *SamSam Ransomware*, May 1, 2018, https://perma.cc/3LAT-VGGV.

deemed affordable. The rate charged to decrypt one system is set at around $10,000, while all systems on the network can be decrypted for $50,000. The group has even offered to decrypt one non-essential system for free to demonstrate their ability and willingness to release the data if their demands are met. The following sections of this article consider whether the SamSam ransomware attacks were internationally wrongful acts and how the United States might legally respond.

3. INTERNATIONALLY WRONGFUL ACTS

For a cyber operation to constitute an internationally wrongful act, it must be attributed to a State and must breach an international obligation owed by that State to another State.[28] Setting aside the question of attribution for the moment, this article first explores whether the SamSam attacks were breaches of an international law obligation. In the context of cyber operations, the most relevant obligations are the prohibition on the use of force, the prohibition on intervention, respect for the sovereignty of other States, and due diligence. Each obligation is examined in detail.

A. Breach of International Obligation

1) Use of Force

The SamSam ransomware attacks were not breaches of the prohibition on the use of force because the scale and effects of the attacks were neither sufficiently severe, immediate, direct, invasive, nor measurable to be considered uses of force. Nor were the SamSam ransomware attacks prohibited threats to use force because although the demands for ransom payments were communicative in nature, the action threatened in the messages was not itself an unlawful use of force.

The United Nations Charter ("U.N. Charter") prohibits the threat or use of force by one State against the territorial integrity or political independence of another.[29] The threshold for what constitutes the use of force in cyberspace is unsettled. However, the prohibition of the use of force is not limited to simply uses of kinetic force. There was general agreement amongst the International Group of Experts (the "Experts") involved in drafting the *Tallinn Manual 2.0* that cyber operations causing death, destruction, injury, or damage are uses of force. Nevertheless, the level of damage inflicted must not be more than de *minimis*.[30]

Whether a cyber activity crosses the use of force threshold can be determined by applying a scale and effects test. The test considers how widespread and of what nature the effects of the cyber activities are. Crucial to the determination is whether

28 Int'l Law Comm'n, Responsibility of States for Internationally Wrongful Acts, G.A. Res. 56/83 annex, U.N. Doc. A/RES/56/83, art. 2 (December 12, 2001) [hereinafter Articles on State Responsibility].
29 U.N. Charter art. 2(4).
30 TALLINN MANUAL 2.0, *supra* note 17, at 334.

the effects of the cyber activities are comparable to those of a kinetic action or a non-kinetic action that qualifies as a use of force. If the activity's effects are comparable, then the cyber activity can also be considered a use of force. If not, the activity is unlikely to qualify as a use of force.

The *Tallinn Manual 2.0* proposes that States are likely to consider eight factors: severity, immediacy, directness, invasiveness, measurability of effects, military character, State involvement, and presumptive legality.[31] Severity is the most important factor. If the scope, duration and intensity of the effects of a cyber activity are severe, it will be likely be considered by States to be a use of force.[32] All the other seven factors are contextual. The more immediate, direct, invasive, measurable, presumptively legal, military in nature, and involving a State the effects are, the more likely it is that the activity will be judged a use of force. Immediacy concerns the time between the cyber activity and its effect.[33] Directiveness involves the nexus between the activity and its effect.[34] Invasiveness describes the activity's degree of penetration into the cyber system of the victim, with the caveat that highly invasive activities that merely exfiltrate data without causing damage will be considered internationally lawful acts of cyber espionage, not uses of force.[35] Measurability of effects gauges the quantifiability of the effects and is linked to the severity factor.[36] Military character is considered relevant because the U.N. Charter is especially concerned with military actions.[37] Presumptive legality is premised on the Lotus principle that international acts not expressly forbidden are permitted.[38] Thus, absent express treaty or accepted custom to the contrary, several prominent cyber activities are presumptively judged not to be uses of force: psychological operations, dissemination of propaganda, espionage, and economic coercion.[39] State involvement, finally, concerns the nexus between the State and the activity.[40] States are also likely to take into account a prevailing political environment, including the relationship between the victim State and the State to which the cyber activity is attributed, when judging whether a cyber activity is a use of force.

31 *Id*. at 334–36.
32 *Id*. at 334.
33 *Id*.
34 *Id*.
35 *Id*. at 334–35. Most scholars agree that peacetime espionage is not the breach of an international obligation, but several has disagreed. *See*, *e.g*., Ingrid Delupis, *Foreign Warships and Immunity for Espionage*, 78 AM. J. INT'L L. 53, 67 (1984) (reasoning that peacetime espionage is illegal under international law if it involves an intrusion of foreign territory); Manuel R. Garcia-Mora, *Treason, Sedition and Espionage as Political Offenses Under the Law of Extradition*, 26 U. PITT. L. REV. 65, 79–80 (1964) (labeling peacetime espionage "an international delinquency and violation of international law"); Quincy Wright, *Legal Aspects of the U-2 Incident*, 54 AM. J. INT'L L. 836, 849 (1960) (stating that peacetime espionage is an "illegitimate enterprise[] because [it] manifest[s] a lack of respect for foreign territory").
36 TALLINN MANUAL 2.0, *supra* note 17, at 335–36.
37 *Id*. at 336.
38 S.S. Lotus (Fr. v. Turk.), Judgment, 1927 P.C.I.J. (ser. A) No. 10, at 3, 18 (Sept. 7).
39 TALLINN MANUAL 2.0, *supra* note 17, at 336.
40 *Id*.

Even assuming that the SamSam incidents can be attributed to a State actor, it is unlikely that their scale and effects are such that they should be considered at least uses of force. Crucially, their overall severity was low. While the potential for serious harm to result from the disruption of normal hospital and municipal functions is high, in none of the incidents did such harm actually occur. The consequences of the SamSam attacks did not follow immediately from the cyber activities. In most cases, the penetration of the affected systems occurred weeks before the ransom notice was directed to the victim, and monetary costs incurred by the victims to recover data and restore their systems followed weeks or months thereafter. Nor were the effects of the SamSam attacks directly connected to the underlying cyber activity. While the attacks did have indirect consequences, in the form of the costs incurred to restore backed-up data and to implement improved security, the directness of the attacks' causes and effects is in no way comparable to the direct harm caused to people or objects by an explosion. Gold Lowell did indeed invasively probe the networks of municipal governments and healthcare providers; however, these were not top-secret networks that were necessarily intended to have the highest level of security. And the networks that the hackers did access were not amongst the most secure maintained by the victims: for instance, Atlanta's emergency response networks were untouched. The effects of the SamSam attacks cannot be calculated with certainty, even if a numerical sum can be affixed to the remediation costs. There is no suggestion that the attacks had a military character: no link has been publicly asserted between the hackers and the military of any State, nor were American military forces the target of the ransomware campaign. Likewise, no State is publicly alleged to have been involved, either directly or indirectly, in the campaign. Finally, the reconnaissance and network probing activities of the Gold Lowell group are qualitatively similar to espionage activities, which are not per se regulated under international law and are not presumptively judged to be uses of use. On consideration of each one of the foregoing factors, the SamSam attacks fail to meet the criteria of a use of force.

Finally, the U.N. Charter prohibits not only unlawful uses of force but also threats of the use of unlawful force.[41] The elements of a prohibited threat of the use of force include that the threat be communicated to the victim and that the threatened action be an unlawful use of force. The *Tallinn Manual 2.0* considers a cyber activity to be a prohibited threat of the use of force when "the threatened action, if carried out, would be an unlawful use of force".[42] The SamSam attacks do involve the communication of a threat that if a ransom is not paid, the victim's data will be lost. But, following the analysis of the previous paragraph, the threatened action is not a use of force. Moreover, by the time Gold Lowell communicated the ransom notice to its victims, it had already undertaken the action of encrypting their files, causing an effect. The group was simply offering the chance to mitigate the effects of its action for a price.

41 U.N. Charter art. 2(4).
42 TALLINN MANUAL 2.0, *supra* note 17, at 338.

The SamSam incidents were neither unlawful uses of force nor unlawful threats of the use of force.

2) Intervention

A cyber activity that falls below the threshold of a use of force may still be a breach of the customary international law principle of non-intervention. In the cyber context, the principle of non-intervention prohibits "coercive intervention, by cyber means, by one State into the internal or external affairs of another".[43] Thus, an intervention consists of two elements: a cyber activity relating to the internal affairs or external affairs of the target State, and the activity must be coercive.

A State's internal affairs or *domaine réservé* comprises those matters "in which [it] is permitted by the principle of sovereignty, to decide freely".[44] In particular, a State's *domaine réservé* includes the "choice of a political, economic, social, and cultural system, and the formulation of foreign policy".[45] According to the *Tallinn Manual 2.0*, the State's choice of political system and its organization lie most clearly within a State's *domaine réservé*.[46] Excluded from a State's *domaine réservé* are all matters that the State has committed to international law. For example, a State bound by human rights obligations that severely restricted the freedom of speech of its citizens could not argue that a cyber operation by another State enabling the first State's citizens to communicate more freely was an unlawful intervention in its *domaine réservé*. By entering into a human rights treaty, the first State had committed such matters to international law and removed them from its *domaine réservé*. In addition to *domaine réservé*, the principle of non-intervention also protects the external affairs of the target State. Thus, matters such as the State's choice of diplomatic and consular relations, recognition of foreign States and governments, membership of international organizations and participation in the drafting of or entry into treaties are all protected. A cyber operation coercively interfering in the *domaine réservé* or the external affairs of the target State is a breach of the principle of non-intervention.[47]

The second component in an unlawful intervention is that it be coercive.[48] While its coercive effect may be indirect, the act must be designed to deprive the target State of the freedom of choice in either its *domaine réservé* or external affairs. The intervening State's action must intentionally cause the target to either act in a way it would otherwise not act or refrain from acting in the manner that it otherwise would have. The mere threat of action can meet the threshold of intervention if it coerces the target State into acting or refraining from action.

43 *Id*. at 312.
44 *Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.)* [hereinafter Nicaragua], Judgment, 1986 I.C.J. 14 (June 27), para 205.
45 *Id*., para. 205.
46 TALLINN MANUAL 2.0, *supra* note 17, at 315.
47 *Id*. at 317.
48 *Nicaragua*, 1986 I.C.J. 14, para. 205 ("The element of coercion . . . defines, and indeed forms the very essence of prohibited intervention.").

The SamSam attacks were not coercive interventions in the *domaine réservé* or external affairs of the United States. There is no suggestion that the SamSam incidents in any way involved the external affairs of the United States, but certain SamSam attacks did implicate its *domaine réservé*. For example, the conduct of the Atlanta traffic police or the operation of the Colorado Department of Transportation are certainly fields of activity not committed to international law. It is less likely that the attacks were coercive efforts designed to influence outcomes in those fields of activity.[49] While Gold Lowell may have manipulated hospitals and municipal governments into making a choice between paying a ransom or spending considerably more to remedy the effects, that choice was not coercive in the sense that it was designed to compel the United States to adopt a particular policy with regard to traffic police, hospitals, or municipal policy. Instead, the coercion was intended to compel the payment of ransom.

3) Violation of Sovereignty

While neither violations of the use of force nor prohibited interventions, the SamSam ransomware incidents, if attributable to a State, were violations of U.S. sovereignty because they caused severe losses of functionality and interfered with the performance of inherently governmental functions. "Sovereignty in the relation 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".[50]

A violation of sovereignty may take one of two forms: a violation of the territorial State's borders or an interference or usurpation of an inherently governmental function of the territorial State. The violating action must be undertaken by or attributable to another State.[51] In cyberspace, a violation of territorial integrity is difficult to identify, especially if the cyber activity is conducted remotely. The *Tallinn Manual 2.0* approach judges whether a violation of territorial integrity is a violation of sovereignty on the basis of "the degree of infringement upon the target State's territorial integrity".[52] Causing physical damage within the territorial State is a violation of sovereignty; causing a loss of functionality to the cyber infrastructure of the territorial State may sometimes be.[53] For instance, the 2012 Shamoon virus, which caused thousands of computers maintained by Saudi Arabia's state oil company to malfunction to the point of necessitating their repair or replacement, was a violation of Saudi Arabia's sovereignty, assuming it could be attributed to a State.[54] A cyber activity that necessitates reinstallation of the operating system would likewise be a

49 TALLINN MANUAL 2.0, supra note 17, at 318 ("[M]ere coercion does not suffice to establish a breach of the prohibition of intervention [. . . . Instead,] the coercive effort must be designed to influence outcomes in, or conduct with respect to, a matter reserved to a target State.").

50 Island of Palmas (Neth. v. U.S.), 2 R.I.A.A. 829 (Perm. Ct. Arb. 1928).

51 TALLINN MANUAL 2.0, *supra* note 17, at 17.

52 *Id*. at 20.

53 *Id*.

54 *Id*. at 21.

violation.[55] However, whether a cyber activity that causes neither physical damage nor a loss of functionality constitutes a breach of the territorial State's sovereignty is unclear.[56]

An interference with or usurpation of an inherently governmental function of the territorial State, regardless of whether damage is caused, also qualifies as a violation of sovereignty.[57] The territorial State enjoys the exclusive right to perform inherently government functions—e.g., delivering social services, conducting elections, collecting taxes, and conducting diplomacy. Inherently governmental function is a narrower concept than *domaine réservé*: whereas the latter concerns an area over which the State has exclusive control, the former deals with specific State functions. Stealing money from a State tax collector is not an interference with or usurpation of the State's inherently governmental tax collection function, whereas preventing the State from collecting taxes or usurping its authority to collect taxes is.

The SamSam ransomware attacks, if attributable to a State, are violations of the sovereignty of the United States. While the attacks did not cause physical damage, they resulted in severe losses of functionality. Medical services were disrupted. Municipal offices were forced offline for weeks. The loss of functionality required spending considerable sums of money to remedy. Moreover, the SamSam incidents also interfered with the performance of inherently governmental functions. Atlanta's court and police operations are inherently governmental functions, which although not usurped were certainly interfered with. Thus, the attacks were violations of the United States' sovereignty and, if attributable to a State, constitute internationally wrongful acts.

4) Due Diligence

The SamSam attacks may also have been breaches of the international obligation of due diligence if the State controlling the territory from which they were launched had a requisite level of knowledge about their occurrence and failed to take feasible actions to prevent them. A territorial State is in breach of its international due diligence obligation to a target State when it has actual or constructive knowledge of and fails to take feasible measures to stop an action affecting the rights of and causing serious adverse consequences to the target State emanating from within the territorial State's territory.[58] In the cyber context, a State must exercise due diligence in not allowing territory under its control to be used for cyber operations that affect the rights of and cause severe adverse consequences to another State.[59]

Breaches of the duty of due diligence do not require that the act in question be

55 *Id*.
56 *Id*.
57 *Id*.
58 *See Corfu Channel (UK v. Alb.)*, 1949 I.C.J. 4, 22 (Apr. 9).
59 TALLINN MANUAL 2.0, *supra* note 17, at 30.

attributable to a State. Instead, the duty of due diligence assumes the role of three parties: the target State toward which the cyber operation is directed; the territorial State; and a third-party author of the cyber operation.[60] The third party may be another State, a non-State group, or a private person. Thus, if the State that controls the territory from which the Gold Lowell group is operating has knowledge of those operations, the operations affect the rights of and cause serious adverse consequences to the United States, and the United States intimates that the State take action to stop the breach of an international norm, that State has a duty to take feasible action to stop the SamSam actions. While the harm caused by a cyber activity must be serious, the due diligence principle does not require that there be physical damages to objects or injuries to persons.[61]

The SamSam ransomware incidents affected the U.S. sovereign right to perform inherently governmental functions – operating courts and police departments. It is questionable, however, whether there were serious adverse consequences. While the incidents certainly had the potential to cause serious adverse consequences – if, for example, the encryption of medical files had led to improper medical care resulting in injury to or death of patients – no such serious adverse consequences were reported.[62]

Knowledge, actual and constructive, is a constitutive element of the duty of due diligence. A State is in breach if even if it is unaware of cyber activity conducted from its territory but "objectively should have known that its territory was being used".[63] There is too little publicly available information to determine whether the State from whose territory the Gold Lowell group is operating actually knows or objectively should know about its operations or whether any actions have been taken to stop the SamSam ransomware attacks. Thus, the analysis need not go further.

B. Attribution

To constitute an internationally wrongful act, the SamSam ransomware attacks must not only be breaches of an international obligation owed by one State to another but must also be attributable to the former. Attribution is especially difficult in cyberspace.[64] A cyber operation is attributable to a State when it is carried out by organs of that State or by organs of another State placed at its disposal. A cyber operation can also be attributed to a State when it is carried out by non-State actors pursuant to the State's

60 *Id*. at 32.
61 *Id*. at 37–38.
62 *See, e.g.*, Duncan, *supra* note 7 (quoting a Baltimore doctor as saying "while things have moved more slowly, patients were getting treated"); Ryckaert, *supra* note 10 ("Life support and other critical hospital services were not affected, and patient safety was never at risk.").
63 TALLINN MANUAL 2.0, *supra* note 17, at 41.
64 *See, e.g.*, William Banks, *State Responsibility and Attribution of Cyber Intrusions After Tallinn 2.0*, 95 TEX. L. REV. 1487, 1505–08 (2017); Christian Payne & Lorraine Finlay, *Addressing Obstacles to Cyber-Attribution*, 49 GEO. WASH. INT'L L. REV. 535, 559–566 (2017). *See also* Thomas Rid & Ben Buchanan, *Attributing Cyber Attacks*, 38 J. STRAT. STUD. 4, 7 (2015) (proposing a "Q model" for attribution, combining tactical, operational, and strategic aspects).

instructions or under its direction or control, or when the State acknowledges and adopts the operation as its own. From the publicly available evidence, it appears that the SamSam attacks cannot be attributed to a State actor because they were not the acts of a State organ, acknowledged and adopted by a State, or carried out by Gold Lowell pursuant to a State's instructions or under a State's direction or control.

1) Attribution of Acts by State Organs and State Organs Placed at the Disposal of Another State

The law of State responsibility defines "organs of a State" broadly to include any State organ, whether it exercises legislative, executive, judicial or any other functions, whatever its position in the organization of the State, and whatever its character as an organ of the central or regional government of the State.[65] An organ of a State also includes "any person or entity which has that status in accordance with the internal law of the State".[66] Thus, if the SamSam attacks were carried out by any governmental unit of a State or if the attackers were a State organ under the State's internal laws and the attacks are found to be breaches of an international obligation owed to the United States, each attack is an internationally unlawful act. However, there is no suggestion in any of the public reporting concerning the SamSam incidents that Gold Lowell is a State organ. No formal announcement has been made to that effect, which contrasts with charges made by the United States against North Korea in the aftermath of the WannaCry malware in 2017.[67] Without further information, it is speculative to presume that Gold Lowell is an organ of any State.

2) Attribution of Acts by Non-State Actors

Even if Gold Lowell is not a State organ, its actions may be attributable to a State if conducted pursuant to that State's instructions or under its direction or control or retroactively acknowledged and adopted.[68] No State has acknowledged and adopted the SamSam attacks. Thus, to attribute the campaign to a State, it must be shown that Gold Lowell was "acting on the instructions of, or under the direction or control of, [a] State".[69]

When a non-State actor is acting upon the instructions of a State, the analysis is simple. If the non-State actor functions as the State's "auxiliary", its actions are attributable to the State.[70] For instance, if a State hires a group of hackers to identify vulnerabilities in an adversary's cyber infrastructure, the group's actions are attributable to the State. Whether a non-State actor is under the "direction or control" of a State is less straightforward. Direction indicates a longer-term relationship between the State

65 Articles on State Responsibility, *supra* note 28, art. 4(1).
66 *Id*., art. 4(2).
67 *See* Michael Schmitt & Sean Fahey, *WannaCry and the International Law of Cyberspace*, JUST SECURITY, Dec. 22, 2017, https://perma.cc/QJ7W-GY7K.
68 *See* TALLINN MANUAL 2.0, *supra* note 17, at 94.
69 Articles on State Responsibility, *supra* note 28, art. 8.
70 TALLINN MANUAL 2.0, *supra* note 17, at 95.

and the non-State actor, and control indicates that the State exercises a high degree of control over the non-State actor's actions. Together, direction and control can be likened to the notion of "effective control" devised by the International Court of Justice in *Nicaragua* and reiterated in *Genocide*.[71] In the cyber context, a State having "effective control" over a non-State actor would determine the execution and course of the cyber operation carried out by the non-State actor and would have authority to order its commencement and cessation.[72] Simply participating in the planning and supervision of non-State actor's cyber operation is not exercising "effective control". Nor is the mere provision of financial or other support.[73]

The SamSam attacks are not attributable to another State because Gold Lowell, according to public sources of information, was not acting under the instruction or "effective control" of another State. Without State attribution, it is impossible to establish that the SamSam incidents constitute an internationally wrong act on the basis of a breach of the prohibition on the use of force, an unlawful intervention, or a violation of U.S. sovereignty. Although it was judged that the SamSam incidents neither constituted a use of force nor a prohibited intervention, they were violations of sovereignty. However, because the actions of the Gold Lowell group cannot be attributed to a State, those violations alone do not constitute internationally unlawful acts. The principle of due diligence does not require that the underlying wrongful action be attributable to a State. Thus, if the State controlling the territory from which the attacks were launched had a requisite level of knowledge and failed to take feasible actions to prevent them, it breached of its duty of due diligence.

4. POSSIBLE RESPONSES

Having established that the SamSam attacks, according to public information, do not meet the criteria of an internationally unlawful act, this section examines the options available for the United States to take in response. Cyber operations may, in general, be met with four responses under international law: countermeasures, the plea of necessity, self-defense, and retorsion. For the reasons explained below, only retorsion is suitable.

A. Countermeasures

Countermeasures are actions are would be unlawful but for the fact that they are taken in response to another State's internationally wrongful act and are designed to terminate that unlawful act or compel the State to which it is attributable to make reparations.[74]

71 *Nicaragua*, 1986 I.C.J. 14, para. 115; *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosn. and Herz. v. Serb. and Montenegro)*, Judgment, 2007 I.C.J. Rep. 108 (Feb. 26), para. 400.

72 TALLINN MANUAL 2.0, *supra* note 17, at 96.

73 *Nicaragua*, 1986 I.C.J. 14, para. 115.

74 Articles on State Responsibility, *supra* note 28, art. 49.

However, the object of countermeasures must be a State,[75] and it is not possible to attribute the SamSam attacks to a State. Moreover, there must be an internationally wrongful act to justify countermeasures.[76] Even if there was, countermeasures should be limited to ensuring that the unlawful act stops, potentially obtaining assurance and guarantees of non-repetition from the responsible State,[77] and compelling the responsible State to make reparations.[78] Because the SamSam incidents have stopped, countermeasures would have to be limited to compelling the responsible State to guarantee that the incidents not resume and providing compensation for damages. Countermeasures may not be punitive or have a retaliatory effect.[79]

Additionally, the United States would be advised not to engage in countermeasures in response to the SamSam attacks even were they attributable to a State because if the countermeasures were to violate a legal obligation owed to a third State, the United States would itself be in breach of international law. The wrongfulness of such a breach is not precluded by the validity of the countermeasure against the responsible State.[80] Thus, the United States could find itself in breach of its international law obligations by too aggressively seeking to curtail Gold Lowell's campaign.

B. Plea of Necessity

The plea of necessity allows a State to act in exceptional cases when there is grave and imminent peril to an essential interest of the State and action is the sole means of safeguarding that interest.[81] Even then, the plea of necessity requires that the injured State's action be balanced with the interests of any States that would be affected and with those of the international community.[82] The injured State's action may not seriously impair the essential interests of affected States.[83] The plea of necessity is not available to injured State that have substantially contributed to their own injury.[84] However, the plea of necessity can be asserted to take action against non-State actors and can justify actions that violate the rights of non-responsible States, if the threat to an essential interest of the injured State is sufficiently grave and imminent and no other means of safeguarding the interest are present. State attribution is not a precondition for action based on the plea of necessity.

A State's "essential interest" is not clearly defined. It would certainly include healthcare, justice, and policing. Thus, the SamSam attacks on healthcare service providers and

75 TALLINN MANUAL 2.0, *supra* note 17, at 112.
76 *Id*. at 114.
77 *Id*. at 142–44 (discussing the responsible State's duty to cease an internationally wrongful act and, if appropriate, provide assurances and guarantees of non-repetition).
78 *Id*. at 144–52 (discussing the responsible State's obligation to make full reparation for injuries suffered by the injured State).
79 Michael N. Schmitt, *"Below the Threshold" Cyber Operations: The Countermeasures Response Option and International Law*, 54 VA. J. INT'L L. 697, 714 (2014).
80 TALLINN MANUAL 2.0, *supra* note 17, at 133.
81 Articles on State Responsibility, *supra* note 28, art. 25(1)(a).
82 *Id*., art. 25(1)(b).
83 *Id*.
84 *Id*., art. 25(2)(b).

Atlanta's police and court systems certainly impaired essential interests of the U.S. It is unlikely that the temporary interruption in functionality the ransomware caused was sufficient to put those essential interests in grave and imminent peril and that no other means existed to safeguard those interests. In any case, the ransomware attacks have abated, if temporarily, and the plea of necessity could only be invoked to end the harmful activity.

C. Self-defense

A State may respond with force to a cyber operation that qualifies an "armed attack" pursuant to the customary international law right of self-defense, codified in Article 51 of the U.N. Charter. Most commentators consider only grave uses of force – typically, those that kill or injure persons or damage or destroy property—to be armed attacks.[85] The U.S., however, takes an outlier position, consistently arguing that any use of force is an armed attack.[86] In *Nicaragua*, the I.C.J. identified "scale and effects" as criteria upon which to judge whether a use of force constitutes an armed attack. In the Court's view, only "the most grave" uses of force do so.[87] Thus, only cyber operations that kill persons or cause significant damage to, or destruction of, property would constitute armed attacks.[88] Because the SamSam ransomware campaign fails to meet the criteria of use of force, even accepting the United States' outlier opinion, it was not an armed attack triggering the right to self-defense.

D. Retorsion

Retorsion, "lawful retaliation in kind for another country's unfriendly or unfair action",[89] is the best legal response available to the United States in dealing with the SamSam attacks. Acts of retorsion are lawful, albeit unfriendly.[90] For example, a State may respond to another State's unfriendly or unfair action by suspending diplomatic relations with the responsible State, restricting travel rights or expelling foreign nationals of the responsible State, or preventing the use of its cyber infrastructure for communications from the responsible State.[91] Retorsion is only way for the United States to respond to the SamSam ransomware campaign without a determination that another State has breached an international obligation owed to it.

5. CONCLUSION

The SamSam ransomware campaign disrupted healthcare organizations and municipal services in numerous locations across the United States. Undoubtedly, the attacks

85 *Nicaragua*, 1986 I.C.J. 14, para. 95.
86 US Department of Defense, Office of the General Counsel, Law of War Manual (June 2015), paras. 1.11.5.2, 16.3.3.1.
87 *Nicaragua*, 1986 I.C.J. 14, para. 191.
88 TALLINN MANUAL 2.0, *supra* note 17, at 341.
89 Black's Law Dictionary (10th ed. 2014).
90 TALLINN MANUAL 2.0, *supra* note 17, at 112.
91 *Id*.

were malicious cyber operations carried out by foreign actors, implicating the rights of the United States under international law. To be considered internationally unlawful acts, the ransomware attacks would have to constitute the breach of an international law obligation owed to the United States and be attributed to a State. The attacks were neither uses of force nor coercive interventions in the *domaine réservé* of the United States. While violations of U.S. sovereignty, the attacks are not attributable to a State according to publicly available reporting. Likewise, it is unknown whether the United States has asked any State to fulfil its due diligence obligation to use all feasible measurable to end the attacks. Thus, the SamSam attacks do not qualify as internationally unlawful acts, limiting the possible recourse for the United States. Even if the ransomware attacks could be attributed to a State, countermeasures would be ill-advised because they would be limited to forcing a State to comply with its legal obligation. Because the attacks are not presently ongoing, the United States would risk engaging in punitive or retaliatory action, for which countermeasure are not allowed. The plea of necessity likewise cannot be invoked to respond to action that has stopped. Because the ransomware was not a use of force, the United States cannot invoke its customary law and Article 51 right of self-defense. Thus, retorsion is the best response available to the United States.