American University International Law Review

Volume 38 | Issue 1 Article 6

2023

Ransomware Groups on Notice: U.S. Cyber Operation Against REvil is Permissible Under International Law

Justin Singh

RANSOMWARE GROUPS ON NOTICE: U.S. CYBER OPERATION AGAINST REVIL IS PERMISSIBLE UNDER INTERNATIONAL LAW

JUSTIN SINGH*

The continued increase in the use of ransomware by cyber criminals has had a costly impact on businesses and organizations around the world. Ransomware groups continue to initiate attacks on businesses and organizations, and states have become increasingly concerned over the potential impact it may have on their critical infrastructure and economies. The United States' recent acknowledgement of cyber operations against ransomware groups highlights the seriousness of the issue and exposes areas of international law that are complicated when applied to cyber operations against these groups. This Comment explores the relevant international law as it applies to the United States and the cyber operation against the criminal ransomware group REvil in the summer of 2021.

The relevant international law as it relates to a cyber operation from the United States is the U.N. Charter's Article 2(4) prohibition on the use of force, the prohibition on intervention under customary international law, and the role of sovereignty. In application to the U.S. operation against REvil, the operation is permissible under international law. It is recommended that the U.S. bolster its legal position by clarifying, promoting, and consolidating its position on the role of sovereignty in international law and its application to cyberspace operations.

* Justin Alexander Singh is a Juris Doctor candidate at American University's Washington College of Law in Washington, D.C., where he is expected to graduate in May 2023. He focuses on areas of the law that intersect with challenges to security, privacy, and technology. The author would like to give special thanks to Professor Gary P. Corn, Program Director of the law school's Tech, Law & Security Program, for his expertise and guidance on the material and throughout the comment writing process.

I. INTRODUCTION

The emergence of the internet and its development into cyberspace has created exceptional new ways for people and organizations to become more collaborative and efficient.[1] Given a growing reliance on connected technologies in cyberspace to communicate and be productive, criminal groups have increasingly employed new tactics to make financial gains.[2] Specifically, the use of "ransomware" by criminal groups has temporarily disrupted operations at a growing

1. *See generally* Kristen Purcell & Lee Rainie, *Technology's Impact on Workers*, PEW RSCH. CTR. (Dec. 30, 2014), https://www.pewresearch.org/internet/2014/12/30/technologys-impact-on-workers (explaining a study about the role of digital technology in professional life).

2. *See Ransomware: Facts, Threats, and Countermeasures*, CTR. FOR INTERNET SEC., https://www.cisecurity.org/insights/blog/ransomware-facts-threats-and-countermeasures, (last visited Feb. 12, 2022) (discussing the threat ransomware poses to U.S. businesses and individuals); *What is Ransomware?*, CHECKPOINT, https://www.checkpoint.com/cyber-hub/threat-prevention/ransomware, (last visited Feb. 12, 2022) (explaining that ransomware groups often seek money or other financial benefits by extorting victims for access to their data).

number of businesses around the world.[3]

Ransomware refers to a type of malware[4] that is used to infect a computer or computer network and attempts to encrypt or otherwise block the victim from accessing data on their computer or network.[5] The victim will traditionally need to pay a ransom to the criminal who infected their computer with ransomware to restore access to their data.[6]

States in the international system have increasingly devoted resources to developing cyber-components in their national defense organizations.[7] In the face of increasing ransomware attacks, states,

---

3. *Ransomware: Facts, Threats, and Countermeasures*, *supra* note 2; *What is Ransomware?*, *supra* note 2.

4. *See What is Ransomware?*, *supra* note 2 (defining malware as software that can remove data, damage, or destroy a computer or computer system); *see What is Malware?*, CISCO, https://www.cisco.com/c/en/us/products/security/advanced-malware-protection/what-is-malware.html, (last visited Mar. 5, 2022) (describing malware, how to detect it, and how to protect a network against it).

5. *See Ransomware: Facts, Threats, and Countermeasures*, *supra* note 2 (explaining how ransomware blocks access to a user's system).

6. *See id.* (explaining that after a system is blocked with ransomware, a ransom is usually demanded to regain access to the system, usually $200–$3,000 in bitcoins); *What is Ransomware?*, *supra* note 2; *see* Jonathan Vanian, *Everything to Know About REvil, the Group Behind a Big Ransomware Spree*, FORTUNE (July 7, 2021), https://fortune.com/2021/07/07/what-is-revil-ransomware-attack-kaseya (explaining that ransomware groups have successfully targeted large companies such as Kaseya, a U.S. software supplier, Quanta, which is a Taiwanese manufacturer, and JBS, a large global meat supplier in Brazil); *Ransomware: Facts, Threats, and Countermeasures*, *supra* note 2 (also referred to as "criminal ransomware groups" or "ransomware groups"); *see What is Ransomware?*, *supra* note 2 (explaining that ransomware encrypts files and then demands a ransom payment for the decryption key); Sean Lyngaas, *U.S. Officials Believe Russia Arrested Hacker Responsible for Colonial Pipeline Attack*, CNN (Jan. 14, 2022), https://www.cnn.com/2022/01/14/politics/us-russia-colonial-pipeline-hack-arrest/index.html (explaining that a ransomware attack on Colonial Pipeline in 2021 was a significant ransomware attack impacting critical infrastructure); *see* Jonathan Greig, *More Than 30 Countries Outline Efforts to Stop Ransomware After White House Virtual Summit*, ZDNET (Oct. 14, 2021), https://www.zdnet.com/article/30-countries-outline-efforts-to-stop-ransomware-after-white-house-virtual-summit (explaining that the increasing use of ransomware has prompted countries to evaluate how they can respond).

7. *See* Josh Gold, *The Five Eyes and Offensive Cyber Capabilities: Building a 'Cyber Deterrence Initiative'*, NATO CCDCOE (2020) https://www.ccdcoe.org/uploads/2020/10/2020-Josh-Gold-Five-Eyes-and-Offensive-Cyber-Capabilities.pdf (outlining how five countries have spoken publicly about their

such as the United States, may and will use cyber operations to thwart or prevent ransomware attacks from happening.[8] Cyber operations are actions that utilize cyber capabilities to achieve objectives in cyberspace.[9] Since cyber operations are conducted through cyberspace, physical effects are more difficult to visualize as compared with traditional military operations.[10] However, cyber operations nonetheless have similar implications on physical territory.[11]

The international nature of cyber operations, in addition to the

---

offensive cyber systems); *see Cyber Operations Tracker*, COUNCIL FOREIGN RELS., https://www.cfr.org/cyber-operations/, (last visited Mar. 5, 2022) (describing that as states develop their cyber capabilities, they have at times used Cyber operations to achieve particular state objectives); *see* Gen. James E. Cartwright, *Joint Terminology for Cyberspace Operations*, ¶ 15, (Nov. 1, 2010), http://www.nsci-va.org/CyberReferenceLib/2010-11-Joint%20Terminology%20for%20Cyberspace%20Operations.pdf (defining that cyberspace itself refers to the domain of electronics and network systems used to store, modify, and exchange information).

8. *See Summary: Department of Defense Cyber Strategy 2018*, DEP'T DEFENSE, (2018), at 1, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF (last visited Feb. 13, 2022) (outlining the Department of Defense's vision for addressing cyber threats); *Our Mission and Vision*, U.S. CYBER COMMAND, https://www.cybercom.mil/About/Mission-and-Vision/, (last visited Jan. 23, 2022); Julian E. Barnes, *U.S. Military Has Acted Against Ransomware Groups, General Acknowledges*, N.Y. TIMES (Dec. 5, 2021), https://www.nytimes.com/2021/12/05/us/politics/us-military-ransomware-cyber-command.html.

9. *See* Cartwright, *supra* note 7, at ¶ 16 (defining cyberspace operations).

10. *See generally* Gary P. Corn, *Cyber National Security: Navigating Gray-Zone Challenges In and Through Cyberspace in* COMPLEX BATTLESPACES: THE LAW OF ARMED CONFLICT AND THE DYNAMICS OF MODERN WARFARE at 363–64 (Winston S. Williams & Christopher M. Ford eds., 2019) [hereinafter Corn, *Cyber National Security*] (outlining the physical, logical, and social dimensions of cyberspace operations).

11. *See id.* at 363–64 (explaining how the physical locations of hardware and other tangible aspects of cyberspace implicate issues of sovereignty and jurisdiction and that cyber operations are initiated from an originating country. The cyber "payload" which may refer to the communication, signal, or data at use in the cyber operation then travels through the originating country's information infrastructure, which includes physical infrastructure, such as routers, access points, and network lines located throughout the territory to connect it with the global information network); *see id.* at 356, 364 (explaining that once a part of the global information infrastructure, the cyber operation's payload may traverse a number of global access points, going through numerous countries and territories before being correctly routed to the cyber operation's target).

unique characteristics of international criminal ransomware groups, poses several international law considerations.[12] These considerations include Article 2(4) of the U.N. Charter,[13] the prohibition on intervention,[14] and the role of sovereignty.[15] As a member of the international system and founding member of the U.N. Charter,[16] the United States is bound by both the U.N. Charter and principles of state practice that are a part of customary international law.[17]

The U.N. Charter's Article 2(4) prohibits states from using force against another.[18] The prohibition on intervention prohibits states from intervening in a coercive manner in an area reserved for the state.[19] Lastly, sovereignty's role as a rule or principle under international law presents significant implications on the legality of any cyber operation.[20] To understand whether a cyber operation against a ransomware group is permissible under international law, an analysis of the requisite thresholds and characteristics of the U.N. Charter's Article 2(4), the prohibition on intervention, and the role of

12. *See id.* at 365 (explaining how cyberspace differs from traditional physical domains and how that affects military operations).

13. *See* U.N. Charter art. 2, ¶ 4 ("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, or in any other manner inconsistent with the Purposes of the United Nations.").

14. *See Prohibition of Intervention*, MAX PLANCK ENCYCLOPEDIAS OF INTERNATIONAL LAW at ¶ 1 (Philip Kunig ed., 2008) (defining the principle of non-intervention).

15. *See Sovereignty*, MAX PLANK ENCYCLOPEDIAS OF INTERNATIONAL LAW at ¶ 1 (Samantha Besson ed., 2008) (defining the principle of sovereignty).

16. *Preparatory Years: U.N. Charter History*, U.N., https://www.un.org/en/about-us/history-of-the-un/preparatory-years, (last visited Feb. 13, 2022).

17. *See* Paul C. Ney, Jr., General Counsel, Dep't Defense, Remarks at U.S. Cyber Command Legal Conference (Mar. 2, 2020), https://www.defense.gov/News/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference (mentioning the evolving customary international law in the area of cyberspace).

18. U.N. Charter, *supra* note 13.

19. *See* Prohibition of Intervention, *supra* note 14, ¶ 1 (Non-intervention "is only prohibited when it occurs in fields of State affairs which are solely the responsibility of inner State actors, takes place through forcible or dictatorial means, and aims to impose a certain conduct of consequence on a sovereign State").

20. *See* Ney, *supra* note 17 (discussing U.S. policy on cyberspace law); Brian J. Egan, *International Law and Stability in Cyberspace*, 35 BERKLEY J. INT'L L. 169, 171 (2017).

sovereignty must be applied to the specific cyber operation.[21]

In December 2021, the U.S. military acknowledged that it had conducted cyber operations against criminal ransomware groups.[22] The acknowledgement is rumored to have been in reference to unconfirmed U.S. cyber operations against the criminal ransomware group REvil in the Summer of 2021.[23] In applying the relevant international law considerations to the U.S. operation, it was permissible under international law because it was not a prohibited use of force under the U.N. Charter's Article 2(4), was not a prohibited intervention under customary international law, and was an action consistent with the role of sovereignty in international law.

To address these international law considerations and their application to the U.S. operation against REvil, Part II of this Comment provides background on ransomware, cyber operations, and international law.[24] Part III applies U.N. Article 2(4), the prohibition on intervention, and the role of sovereignty to cyberspace and argues that the U.S. cyber operation was not a prohibited use of force or a prohibited intervention, and did not impermissibly violate sovereignty.[25] Part IV recommends that the United States take an explicit position on sovereignty, promote its position to like-minded nations, and advocate for the adoption of its position to multi-lateral organizations.[26] Part V concludes.[27]

---

21. U.N. Charter, *supra* note 13; Prohibition of Intervention, *supra* note 14, at ¶¶ 1–6; *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 17 (Michael N. Schmitt 2d ed., 2017).

22. *See* Barnes, *supra* note 8 (reporting on a General's comment that the U.S. has acted against ransomware groups).

23. *See* Ellen Nakashima & Dalton Bennett, *A Ransomware Gang Shut Down After Cybercom Hijacked Its Site and It Discovered It Had Been Hacked*, WASH. POST (Nov. 3, 2021), https://www.washingtonpost.com/national-security/cyber-command-revil-ransomware/2021/11/03/528e03e6-3517-11ec-9bc4-86107e7b0ab1_story.html (discussing U.S. action against REvil and explaining that the reported operation against REvil by U.S. Cyber Command disrupted and degraded REvil's ability to conduct ransomware operations and eventually led the group to cease their activity voluntarily and temporarily).

24. Background *infra* Part II.

25. Analysis *infra* Part III.

26. Recommendations *infra* PartIV.

27. Conclusion *infra* Part V.

II. BACKGROUND

A. THE RISE OF RANSOMWARE GROUPS

The rise of malign cyber activity has impacted private companies and government infrastructure, costing companies and organizations millions in damages.[28] Ransomware criminal groups have taken on common characteristics as they have continued to emerge.[29] While some criminal ransomware groups have members across the globe, others are concentrated in a particular region and attempt to operate anonymously through global information infrastructure.[30] Although ransomware groups are commonly motivated by financial gain, their objectives can sometimes align with the objectives of state actors who may, in turn, sponsor or encourage a ransomware group's activities.[31]

In achieving their objectives, ransomware groups will attempt to gain unauthorized access to a target victim's computer or network.[32] Once the group is satisfied with the level of access they have achieved for the target, the group will distribute ransomware to the

---

28. *See* William Turton & Kartikay Mehrotra, *Notorious Russian Ransomware Group 'REvil' Has Reappeared*, BLOOMBERG (Sept. 7, 2021), https://www.bloomberg.com/news/articles/2021-09-07/notorious-russian-ransomware-group-revil-has-reappeared (discussing the re-emergence of REvil); Vanian, *supra* note 6; *see Ransomware: Facts, Threats, and Countermeasures*, *supra* note 2 (explaining the use of ransomware in particular has become threatening through its use by cyber-criminal groups that employ sophisticated strategies to extract ransoms from their victims in exchange for returning access of data and systems).

29. *See What is Ransomware?*, *supra* note 2 (outlining common features of ransomware).

30. *See id.* (explaining how ransomware groups differ in their composition, and explaining that ransomware groups additionally have a spectrum of technical sophistication from a basic level that go after "easy" targets, to groups that have exceptional capabilities that leverage complex exploits).

31. *See* Frank Bajak, *How the Kremlin Provides a Safe Harbor for Ransomware*, AP NEWS (Apr. 16, 2021), https://apnews.com/article/business-technology-general-news-government-and-politics-c9dab7eb3841be45dff2d93ed3102999 (explaining how Russia provides support to some ransomware groups).

32. *See* Alexander S. Gillis & Ben Lutkevich, *What is Ransomware?*, TECHTARGET, https://www.techtarget.com/searchsecurity/definition/ransomware, (last visited Feb. 12, 2022) (explaining how ransomware groups obtain access to a computer or network and that once the ransomware group has obtained access, the group will attempt to leverage the compromised device or network's credentials to access as many devices or other networks associated with the compromised device as possible, increasing the number of devices and networks that are compromised).

compromised devices or across the compromised networks.[33]

Ransomware is software, effectively malware,[34] that attempts to install itself on the compromised device or devices on a particular network undetected.[35] Once activated, the ransomware software will lock out the device or network from access by the target and encrypt the data present on the device or network.[36] Once the target has paid the ransom, the ransomware group will send decryption keys that will allow the target to regain access to their devices or network.[37]

Since ransomware groups operate on a global level, often out of several different countries or regions, they operate independently of state actors.[38] Accordingly, operations conducted against ransomware

33. *See id.* (explaining how a ransomware group proceeds to further compromise other devices or networks).

34. *See Ransomware: Facts, Threats, and Countermeasures*, *supra* note 2 (defining that malware refers to software that can remove data, damage, or destroy a computer or computer system).

35. *See* Gillis & Lutkevich, *supra* note 32 (explaining how ransomware attempts to spread undetected, and explaining that after ransomware has been distributed across the compromised networks or devices, the ransomware group can activate it at a time of their choosing so long as they can maintain connectivity to a compromised device or network).

36. *See id.* (explaining how the ransomware will encrypt data, and explaining that ransomware groups will then communicate instructions to the target who owns the devices or network on how to send the desired ransom to the group).

37. *See id.* (discussing what happens after ransom is paid).

38. *See* Elizabeth Merrigan, *Blurred Lines Between State and Non-State Actors*, COUNCIL FOREIGN RELS., (Dec. 5, 2019), https://www.cfr.org/blog/blurred-lines-between-state-and-non-state-actors (discussing how some groups act with state governments and independently at different times); *see* Kellen Dwyer, *It's Time to Surge Resources Into Prosecuting Ransomware Gangs*, LAWFARE, (May 20, 2021), https://www.lawfareblog.com/its-time-surge-resources-prosecuting-ransomware-gangs (arguing that more resources should go into cyberwarfare); Draft Articles on Responsibility of States for Internationally Wrongful Acts, art. 8, U.N. Doc. A/56/10, 43 (2001) [hereinafter Draft Articles] (explaining that only in particular, fact-based circumstances, can ransomware groups be designated as state actors under international law); *see generally* Corn, *Cyber National Security*, *supra* note 10, at 422 (arguing that while the impacts of ransomware operations conducted by criminal ransomware groups may align with the objectives of state actors, ransomware groups are more often viewed as non-state actors. A state must prove the non-state actor was under the instruction or direction or control of another state to be attributed as effectively a state actor; the designation of ransomware groups as non-state actors is an important status as it complicates the applicability of international law. International law is applicable to the actions of non-state actors

groups must be examined in the scope of international law obligations to the state or states in which a cyber operation is expected to be conducted, impact, or traverse vis a vis the state conducting the operation.[39]

B. REVIL AND ITS ORIGINS

REvil, an amalgam of "ransomware" and "evil," (and sometimes referred to as "Sodinokibi") is a notorious criminal ransomware group.[40] States have attributed responsibility to REvil for a number of high-profile ransomware attacks with victims such as Kaseya, JBS, and Quanta.[41] Additionally, REvil and its members are closely associated with the group responsible for the Colonial Pipeline ransomware attack.[42] Outside of conducting and carrying out their own ransomware attacks, REvil authorizes other criminal groups to access their infrastructure[43] to perpetuate malign cyber activity, including ransomware attacks.[44]

REvil is largely considered a Russian ransomware group due to a number of their members reportedly being Russian citizens, or operating from Russia.[45] In addition to REvil's individual associations

---

only during particular circumstances often attributed under *Nicar. v. U.S.,* 1986 I.C.J, 14 ¶ 191 (June 27) and in the absence of these factors does not impose obligations or responsibilities).

39. *See* Egan, *supra* note 20, at 171 (explaining the relationship between international law and potential cyber operations).

40. *See* Vanian, *supra* note 6 (providing background information on REvil); Turton & Mehrotra, *supra* note 28; Dan Mangan et al., *Multiple REvil Ransomware Sites Are Down on the Dark Web*, CNBC (July 13, 2021), https://www.cnbc.com /2021/07/13/multiple-revil-ransomware-sites-are-down-on-the-darkweb-.html.

41. *See* Vanian, *supra* note 6 (introducing Kaseya, which is a large U.S. based business software company, JBS, which is one of the largest global meat suppliers located in Brazil, and Quanta, which is a major Taiwanese hardware supplier).

42. *See* Lyngaas, *supra* note 6 (explaining that the ransomware attack disrupted operations enough to impact the U.S. oil supply along the East Coast); *see* Greig, *supra* note 6 (explaining that in January 2022, U.S. officials indicated that they believed one of the hackers responsible for the attack was arrested during a Russian raid on suspected REvil members).

43. *See* Vanian, *supra* note 6 (explaining that REvil maintains and operates infrastructure on the dark web).

44. *See id.* (explaining that REvil works in exchange for a portion of any ransom or assets the criminal groups receive as a result of using the infrastructure).

45. *What is Ransomware?*, *supra* note 2; Vanian, *supra* note 6; Turton &

with Russia, the Russian government has garnered a reputation for providing an acquiescent environment for ransomware groups to operate from, including REvil.[46] Experts have further accused Russian security services of providing REvil and other cyber-criminal groups with tacit or even explicit consent to operate.[47]

C. U.S. CYBER COMMAND'S ROLE AND MISSION

The U.S. Secretary of Defense directed the creation of U.S. Cyber Command (hereinafter Cyber Command) on June 23, 2009, and subsequently elevated Cyber Command to a combatant command in 2018.[48] Cyber Command's mission is to "Direct, Synchronize, and Coordinate Cyberspace Planning and Operations - to Defend and Advance National Interests - in Collaboration with Domestic and International Partners."[49]

In 2018, the U.S. Department of Defense (DoD) released its Cyber Strategy, which detailed policy approaches to rising threats in cyberspace.[50] As part of that strategy, the DoD claimed that it "will defend forward to disrupt or halt malicious cyber activity at its

---

Mehrotra, *supra* note 28.

46. *See* Bajak, *supra* note 31 (discussing the connection between the Russian government and REvil, and explaining that cyber security experts suggest that there are indications that Russia's security services sometimes employ cyber criminals to work for their government agencies); Barnes, *supra* note 8 (explaining that the United States has previously suggested that Russia has refused to take appropriate measures to stop REvil and similar ransomware groups from operating in the country).

47. Bajak, *supra* note 31; Lyngaas, *supra* note 6; Greig, *supra* note 6 (describing that in January 2022, Russian security services publicly acknowledged that they had conducted a raid on the homes of fourteen people suspected of being members of REvil at the request of U.S. authorities).

48. *Our History*, U.S. CYBER COMMAND, https://www.cybercom.mil/About/History, (last visited Feb. 13, 2022); Jim Garamone, *Cybercom Now a Combatant Command, Nakasone Replaces Rogers*, DEP'T DEFENSE (May 4, 2018), https://www.defense.gov/News/News-Stories/Article/Article/1512994/cybercom-now-a-combatant-command-nakasone-replaces-rogers.

49. Our Mission and Vision, *supra* note 8 (stating that part of Cyber Command's responsibilities include defending the Department of Defense Information Networks, supporting combatant commands, and strengthening the "nation's ability to withstand and respond to cyber-attacks").

50. Summary: Department of Defense Cyber Strategy 2018, *supra note 8*, at 1.

source."[51] The DoD has since conducted cyber operations against ransomware groups, though it has not confirmed which groups it has taken action against.[52]

D. THE U.S. CYBER OPERATION AGAINST REVIL

On December 5, 2021, Commander of Cyber Command, U.S. Army General Paul Nakasone, acknowledged for the first time that the U.S. military had engaged in offensive cyber operations against ransomware groups.[53] The operation was reported to have occurred around September and October 2021 and targeted the servers REvil used to conduct its operations.[54] As part of the reported operation, the U.S. Federal Bureau of Investigation (FBI) and an unnamed partner nation hacked into REvil's servers over the summer of 2021.[55] The FBI and the foreign partner's hack allowed the FBI to gain access to the server and obtain private access keys to the server that it later passed along to Cyber Command.[56]

Using the private access keys obtained by the FBI, Cyber Command was able to access REvil's servers.[57] Cyber Command then used its access to REvil's servers to clone the website that the group used to

---

51. *Id.*

52. Ney, *supra* note 17; *see* Barnes, *supra* note 8 (explaining that where previously the DoD has seen ransomware groups as the responsibility of law enforcement, it has now assumed a larger role in an effort to deter and mitigate the threat posed by criminal ransomware groups by conducting punitive cyber operations against them directly); *see* Egan, *supra* note 20, at 171 (arguing that cyber operations carry important international law considerations, especially where operations or actions will take place on the territory of another state actor, and explaining that even when an operation is a cyber operation, when the operation occurs on another state's territory or its territory is impacted, the United States' international law obligations and responsibilities remain present).

53. Barnes, *supra* note 8; Lyngaas, *supra* note 6; *see* Nakashima & Bennett, *supra* note 23 (explaining that General Nakasone's acknowledgement came just months after reports that Cyber Command had conducted cyber operations against REvil that caused the criminal ransomware group to temporarily shut down its operations).

54. Nakashima & Bennett, *supra* note 23.

55. *See id.*; *Hack*, OED ONLINE (Dec. 2021), https://www.oed.com/view/Entry/83030 (explaining the act of hacking in cyberspace refers to the action of gaining unauthorized access to a network system or computer).

56. *See* Nakashima & Bennett, *supra* note 23.

57. *See id.*

extort its victims and receive ransom.[58] After cloning the website, Cyber Command redirected traffic away from the original, effectively hijacking the group's ability to use the platform to extort their targets and victims.[59] In effect, the operation disrupted REvil's ability to operate.[60] Shortly after the operation, one of REvil's leaders, publicly known online only as "o_neday," acknowledged on a Russian-language forum frequented by cyber criminals that someone had hijacked REvil's domains and compromised its server.[61]

Limited only to public reporting, it is unclear where Cyber Command's communications with REvil's server took place and where the server was located.[62] For purposes of analysis, this Comment assumes REvil's servers were based in Russia and examines the legal implications, the impacts, and the effects of those servers in Russia, although the operation could have involved servers hosted in a third-party state.[63]

E. ARTICLE 2(4): THE PROHIBITION ON THE USE OF FORCE

Since 1945, 189 countries have signed and ratified the U.N. Charter and are therefore bound by its provisions, including its codified principles of sovereign equality of states and the prohibition of the use of force.[64]

---

58. *See id.*

59. *See id.*

60. *See id.* (REvil's operations appeared to completely stop for a period of time); Gary P. Corn & Peter Renals, *Scenarios for Defend Forward*, *in* THE UNITED STATES' DEFEND FORWARD CYBER STRATEGY: A COMPREHENSIVE LEGAL ASSESSMENT, 26–29 (Jack Goldsmith ed., Feb. 2022) (an immunization cyber operation can involve the use of exploits to obtain access into a target server to reconfigure its network protocols to either disrupt or prevent the target from utilizing their server in a malicious manner or benign users from connecting with IT interfaces emanating from the server).

61. *See* Nakashima & Bennett, *supra* note 23 (explaining soon afterward, REvil stopped its operations and effectively shut down voluntarily, and temporarily).

62. *See id.*

63. Corn & Renals, *supra* note 60, at 26–29 (noting a Foreign Malign Influence hypothetical cyber operation illustrates what could be encompassed by the Defend Forward concept and showcases the highly international characteristics inherent in cyber operations with the involvement of third-party states).

64. *See United Nations Charter*, U.N., https://www.un.org/en/about-us/un-charter, (last visited Feb. 13, 2022) (explaining the U.N. organization and structure is created through the U.N. Charter which becomes binding on states through

The prohibition of the use of force is a cornerstone of the international law system and is universally accepted as a norm of customary international law.[65] The prohibition of the use of force is codified in the U.N. Charter's Article 2(4), which requires that all member States "refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."[66] Applying Article 2(4) to non-traditional military actions, such as cyber operations, becomes less clear when compared to traditional military operations——for example, the requisite threshold that a cyber operation must reach to be considered a use of force.[67]

The Tallinn Manual 2.0[68] (hereinafter Tallinn Manual) is consistent with other states in finding that there are varying levels of uses of force.[69] Rule 69 of the Tallinn Manual articulates this approach, finding that a cyber use of force is achieved "when its scale and effects are comparable to non-cyber operations rising to the level of a use of

---

ratification of the Charter as a treaty).

65. *Prohibition of Use of Force*, MAX PLANCK ENCYCLOPEDIAS OF INTERNATIONAL LAW, at ¶ 1 (Oliver Dörr ed., August 2019).

66. U.N. Charter, *supra* note 13.

67. *See Prohibition of Use of Force*, MAX PLANCK ENCYCLOPEDIAS OF INTERNATIONAL LAW, at ¶¶ 1, 20 (Oliver Dörr ed., August 2019) (introducing the principle of prohibition of use of force in international law, and explain among the international community, the difference in terminology denotes two separate meanings whereby "armed attack" in Article 51 sets forth a threshold where a state is justified in using force in its self-defense while "use of force" in Article 2(4) describes a standard for conduct that is prohibited among state actions); Corn, *Cyber National Security*, *supra* note 10, at 405, 409 (stating that within the U.N. Charter, neither the terms "use of force" nor "armed attack" is explicitly defined and their meanings and thresholds are debated within the international community); *See* U.N. Charter, *supra* note 13, art. 51 (justifying a state's use of force when that state defends itself from an armed attack); *Tallinn Manual*, *supra* note 20.

68. *See Tallinn Manual*, *supra* note 20, at 2 (reflecting the opinions of an international group of legal experts and therefore the Tallinn Manual itself is not law but has become a persuasive authority for states in considering the impact and application of international law to cyberspace).

69. *See id.* at 332 cmt. 6–7, 333, cmt. 9 (taking an approach for below the level of an armed attack of applying a series of factors in considering the scale and effects of an operation to determine whether the operation reached the threshold of a use of force).

force."[70] Comment nine to Rule 69 lists the factors that the Tallinn Manual suggests states should consider in determining when a cyber operation reaches the level of a use of force, including severity, immediacy, directness, invasiveness, measurability of effects, military character, state involvement, and presumptive legality.[71] While comment nine emphasizes that these factors are not formal legal criteria, the comment suggests that states should consider the importance of these factors in making a use of force determination.[72]

The U.S. position on Article 2(4)[73] can be understood through the perspective of the DoD. [74] Articulating this perspective, the General Counsel (Paul Ney) for the DoD spoke at the U.S. Cyber Command Legal Conference in March 2020.[75] Mr. Ney stated that in assessing whether a cyber operation conducted by or against the United States constitutes a use of force under Article 2(4), "DoD lawyers consider whether the operation causes physical injury or damage that would be considered a use of force if caused solely by traditional means like a missile or a mine."[76] Under this perspective, a cyber operation rises to the level of a use of force when it has the same impact of death, injury, or destruction as a traditional kinetic or physical operation that meets the threshold of a use of force under Article 2(4).[77]

---

70. *See id.* at 330 (detailing Rule 69 of the Tallinn Manual).

71. *See id.* at 333, cmt. 9 (providing the factors the Tallinn Manual recommends States consider).

72. *Id.*

73. *See Founding Member States*, U.N., https://research.un.org/en/unmembers/founders, (last visited Feb. 13, 2022) (noting that the United States is a founding member and signatory of the U.N. Charter and thus bound by its obligations).

74. *See* Gary P. Corn, *National Security in the Digital Age*, *in* NATIONAL SECURITY LAW AND THE CONSTITUTION, at 915, 958, 962, n. 1 (2020) [hereinafter "Corn, *Nat'l Sec. Digital Age*"] (stating that amongst a small number of states that have produced an official view on international law applicability to cyber operations, Mr. Ney's speech set out the DoD's views, building on previous statements made by U.S. government officials); *Prohibition of Use of Force*, *supra* note 65, at ¶¶ 20, 22; *See also* Ney, *supra* note 17 (providing a framework for legal analysis).

75. *See* Ney, *supra* note 17 (speaking as then General Counsel for the DoD on the applicability of international law to cyberspace, including the recognition that the prohibition on the use of force is applicable to cyber operations).

76. *Id.*

77. *See id.* (considering the capacity of cyber activity to be classified as use of force); Corn, *Cyber National Security*, *supra* note 10, at 409; *Tallinn Manual*, *supra* note 20, at 330 (in this regard, the Tallinn Manual Rule 69 and the U.S. position are

F. THE PROHIBITION ON INTERVENTION

The prohibition on intervention is customary international law.[78] The prohibition of intervention prohibits state actions that impermissibly interfere with the internal systems or foreign policy of a state.[79] A state violates the prohibition on intervention when its conduct impacts another state's *domaine réservé*[80]—areas that are solely reserved to the state—and when the action on the *domaine réservé* is so forcible as to constrain the state from freely acting within areas of its *domaine réservé*.[81]

The *domaine réservé* of a state refers to areas that are solely under the discretion of the state to control.[82] These areas are not governed by treaties, or other international law principles or structures, [83] and are solely reserved to the state.[84] For a state action to be a prohibited intervention, the action must have an impact on one of these areas that are reserved to another state's sole discretion.[85]

In addition to a state's act impacting the *domaine réservé*, the act must be coercive.[86] A coercive act is one that restricts a state's ability to decide freely in an area of its *domaine réservé* through forceful or dictatorial means.[87] Coercion traditionally has been understood as force or the threat of forcible means,[88] but need only to be so dictatorial in its effect as to limit a state's ability to decide freely in its *domaine*

---

consistent, insofar as the use of force threshold for a cyber operation can occur when the operation has the same or similar impact as a non-cyber operation akin to a traditional kinetic operation); *see* Ney, *supra* note 17.

78. *See Prohibition of Intervention*, *supra* note 14, ¶¶ 1–2.

79. *See id.* ¶ 3.

80. *See id.* ¶¶ 3–4 (explainging that *domaine réservé* refers to areas under the sole discretion of a state to determine).

81. *See id.* ¶ 1.

82. *See id.* ¶¶ 3–4.

83. *See id.*

84. *See id.* ¶¶ 1, 3–4 (noting that the *domaine réservé* has often been considered to include areas such as a state's discretion to freely choose and make decisions in areas of its economic, political, or cultural systems and structures and foreign policy).

85. *See id.* ¶¶ 1, 3–4.

86. *See id.* ¶¶ 1, 5–6.

87. *See id.* ¶ 5.

88. *See id.* ¶ 6.

réservé.[89] Determining a coercive act can be difficult, as demonstrated by the 2016 Russian hack of the U.S. Democratic National Committee (DNC) that took place during the U.S. presidential election cycle.[90] Though Russia's hackers hacked the DNC and released its internal emails which consequently impacted the DNC's public support, it is uncertain whether the act met the threshold of coercion.[91]

In its application to cyber operations, a state's cyber operation must meet the same elements of a prohibited intervention.[92] The Tallinn Manual takes a similar approach to the prohibition on intervention.[93] Rule 66 of the Tallinn Manual states that a "State may not intervene, including by cyber means, in the internal or external affairs of another State."[94] Internal and external affairs are defined to be consistent with the concept of *domaine réservé*.[95] The Tallinn Manual is distinguishable, however, in its interpretation of coercion.[96] Under the Tallinn Manual, an act is coercive only when it has a coercive effect

89. *See id.* (expressing that a coercive act does not necessarily require force or a threat of force).

90. *See* Ellen Nakashima & Shane Harris, *How the Russians Hacked the DNC and Passed Its Emails to WikiLeaks*, WASH. POST (July 13, 2018), https://www.washingtonpost.com/world/national-security/how-the-russians-hacked-the-dnc-and-passed-its-emails-to-wikileaks/2018/07/13/af19a828-86c3-11e8-8553-a3ce89036c78_story.html (detailing that Russian government hackers attacked email accounts of staffers in the Clinton administration); *see* Duncan B. Hollis, *Russia and the DNC Hack: What Future for a Duty of Non-Intervention?*, OPINIOJURIS (July 25, 2016), http://opiniojuris.org/2016/07/25/russia-and-the-dnc-hack-a-violation-of-the-duty-of-non-intervention (discussing the hacking of DNC data).

91. *See* Hollis, *supra* note 90; James Andrew Lewis, *Russia and the DNC Hacks*, CTR. STRATEGIC INT'L STUD. (Aug. 15, 2016), https://www.csis.org/analysis/russia-and-dnc-hacks (stating that the Russian hack of the DNC is an effort to shape American politics).

92. *See* Corn, *Cyber National Security*, *supra* note 10, at 413 (for a cyber operation to be recognized as a prohibited intervention under international law, it must have an impact on a state's domaine réservé and it must be coercive to effectively limit the state's ability to decide freely).

93. *See Tallinn Manual*, *supra* note 20, at 314.

94. *See id.* at 312.

95. *See id.* at 314 (stating that the Tallinn Manual Rule 66 comment 6 indicates that reference to internal affairs is consistent with the concept of the domaine réservé of a state, and external affairs referring to relations that are consistent with the sole prerogative of the state, include foreign policy, under comment 16).

96. *See id.* at 318.

and was designed to be coercive in a way to influence or change conduct reserved to be under the discretion of another state.[97] Accordingly, a cyber operation is a prohibited intervention when it impacts an area under a state's *domaine réservé* and the act is so coercive that it limits the state's ability to decide freely in its *domaine réservé*.[98] Under a Tallinn Manual interpretation, the coercive act must also have been designed to be coercive.[99]

G. THE ROLE OF SOVEREIGNTY IN CYBERSPACE

Sovereignty is an immensely important characteristic of international law.[100] State sovereignty has traditionally been understood as a state's supreme authority and has internal and external components.[101] The internal component of sovereignty refers to the state's recognized authority to control its people and things within its territory, while external sovereignty refers to a state's equal rights and obligations to other states in the international system.[102] As it applies to cyberspace, the infrastructure, equipment, data, and communications characteristic of modern information infrastructure fall under the category of a state's internal sovereignty.[103] However, there is tension between the two components of sovereignty in the practical function of state practice.[104] Internal sovereignty of a state to maintain people and things in its territory can clash with another state's external sovereignty-based rights or duties.[105] The tension between these components of sovereignty challenges the legal significance of sovereignty as a rule of international law.[106]

The DoD position on sovereignty is that sovereignty is a principle

97. *See id.* at 318, cmt. 19.
98. *See Prohibition of Intervention*, *supra* note 14, ¶¶ 1–2.
99. *See Tallinn Manual*, *supra* note 20, at 312, 318.
100. *See Sovereignty*, *supra* note 15, ¶ 1.
101. *See id.* at ¶ 70; Corn, *Cyber National Security*, *supra* note 10.
102. *See Sovereignty*, *supra* note 15, ¶ 70.
103. *See* Corn, *Cyber National Security*, *supra* note 10, at 415–16.
104. *See Sovereignty*, *supra* note 15, ¶ 70; Corn, *Cyber National Security*, *supra* note 10, at 416; *see generally Corfu Channel Case* (U.K. v. Alb.), Judgment, 1949 I.C.J. 49, (Dec. 15, 1949).
105. *See Corfu Channel Case* (U.K. v. Alb.), Judgment, 1949 I.C.J. 49.
106. *See* Ney, *supra* note 17; Corn, *Cyber National Security*, *supra* note 10, at 415–16.

and not a rule of international law.[107] The DoD position posits that there is a lack of state practice or opinio juris (custom) to recognize sovereignty as a rule of international law.[108] In support of the DoD position is the law of state responsibility and the holdings of the "Lotus" principle.[109] The law of state responsibility is customary international law[110] that the U.N. articulated in the U.N. Draft Articles on Responsibility of States for Internationally Wrongful Acts.[111] State responsibility holds that states breach international law when the state is attributed to having acted or failed to act in accordance with an international obligation that the state owed.[112] Separately, the Lotus principle refers to the Permanent Court of International Justice (PICJ) decision in the Case of the *S.S. Lotus*—that states are free to engage in all activities that are not expressly prohibited by international law.[113] Taken together, the Lotus principle and the law of state responsibility are used to support the DoD position that cyber operations that interfere with a state's internal sovereignty are permissible under international law because no state practice or international obligation regulates the use of cyber operations below the thresholds of a use of force or prohibited intervention.[114]

However, some states[115] and the Tallinn Manual take the position

---

107. *See* Ney, *supra* note 17; Corn, *Cyber National Security*, *supra* note 10, at 416–17.

108. *See* Egan, *supra* note 20, at 174 (explaining the United States' stance on state sovereignty); Ney, *supra* note 17; Corn, *Cyber National Security*, *supra* note 10, at 416–17.

109. *See* Corn, *Nat'l Sec. Digital Age*, *supra* note 74, at 967.

110. *See* James Crawford, *State Responsibility*, MAX PLANK ENCYCLOPEDIAS OF INTERNATIONAL LAW, ¶¶ 1–2 (James Crawford ed., Sept. 2006).

111. *See State Responsibility*, *supra* note 110, ¶ 3; Draft Articles, *supra* note 38, art. 8 ¶¶ 1–2 (the Draft Articles of State Responsibility were produced by the U.N.'s International Law Committee).

112. Draft Articles, *supra* note 38, art. 8 ¶¶ 1–2; *State Responsibility*, *supra* note 110, ¶ 17; Corn, *Nat'l Sec. Digital Age*, *supra* note 74, at 967.

113. *S.S. Lotus* (Fr. v. Turk.), 1927 P.C.I.J. (ser. A) No. 10 (Sept. 7) ¶¶ 50–53; *The Lotus*, MAX PLANCK ENCYCLOPEDIAS OF INTERNATIONAL LAW, ¶ 15 (Armin von Bogdandy & Markus Rau eds., June 2006).

114. *See The Lotus*, *supra* note 113, ¶ 15; Draft Articles, *supra* note 38, ¶¶ 1–2; Ney, *supra* note 17; Egan, *supra* note 20, at 174; Corn, *Cyber National Security*, *supra* note 10, at 416–17.

115. *See* Corn, *Nat'l Sec. Digital Age*, *supra* note 74, at 969.

that sovereignty is a rule of international law.[116] Rule 4 of the Tallinn Manual states that a "State must not conduct cyber operations that violate the sovereignty of another State."[117] Consequently, the role of sovereignty is contested under international law and as it relates to cyber operations.[118]

III. ANALYSIS

The U.S. cyber operation against REvil implicates several international legal obligations, including the applicability of the U.N. Charter Article 2(4) prohibition on the use of force, the prohibition on intervention, and the role of sovereignty.[119] Under the application of each of these principles and their requisite standards, the U.S. cyber operation against REvil was consistent with and permissible under international law.

A. THE U.S. OPERATION AGAINST REVIL WAS NOT A PROHIBITED USE OF FORCE UNDER ARTICLE 2(4) OF THE U.N. CHARTER BECAUSE THE OPERATION'S EFFECT WAS NOT SIMILAR OR THE SAME AS A TRADITIONAL KINETIC OPERATION.

1. The U.S. Operation Against REvil Was Not a Prohibited Use of Force Under the DoD Position on the Applicability of U.N. Charter Article 2(4).

The U.S. operation against REvil must be below the threshold of a use of force or otherwise justified as a use of force to be permissible

116. *See Tallinn Manual*, *supra* note 20, at 17.

117. *See id.* at 16–17, 31.

118. *See* Egan, *supra* note 20, at 174; Corn, *Cyber National Security*, *supra* note 10, at 416–17; *see* Ney, *supra* note 17 (under the DoD position, sovereignty is a principle of international law, and cyber operations that interfere with a state's internal sovereignty may be permissible under international law); Corn, *Cyber National Security*, *supra* note 10, at 416–17; *see Tallinn Manual*, *supra* note 20, at 13, 16–17 (alternatively, for states that share the Tallinn Manual approach, sovereignty is a rule of international law and cyber operations that violate a state's sovereignty amount to a violation of international law).

119. *See generally* Paul C. Ney, Jr., *Some Considerations for Conducting Legal Reviews of U.S. Military Cyber Operations,* 62 HARV. INT'L L. J. ONLINE 22, (2020) https://harvardilj.org/wp-content/uploads/sites/15/Some-Considerations-for-Conducting-Legal-Reviews-of-US-Military-Cyber-Operations.pdf.

under international law.[120]

Because the United States is a founding member of the U.N. and ratified the U.N. Charter in 1945, it is bound to its provisions, including Article 2(4).[121] Public reporting indicates that at least some of REvil's operations and infrastructure have been based in Russia, and for purposes of analysis, the impact of the U.S. cyber operation will be assessed by its impact in Russia (although it is possible a third-party state could have hosted some of the REvil infrastructure involved in the cyber operation).[122] In this regard, the U.S. cyber operation against REvil would have needed to produce an impact similar to what a traditional kinetic operation would have had on REvil's operating and information infrastructure in Russia to be considered a use of force.[123]

The U.S. operation against REvil reportedly utilized private access keys acquired by the FBI and a foreign nation partner to access the server used for their extortion platform and redirected traffic away from the platform.[124] In applying the DoD position on the use of force, the U.S. operation did not have an impact on REvil's infrastructure

120. *See* U.N. Charter art. 2, ¶ 4; Egan, *supra* note 20, at 171 (stating that the United States has been unequivocally in accord with the belief that existing international law applies to state behavior in cyberspace); *see* Harriet Moynihan, *The Application of International Law to State Cyberattacks*, CHATHAM HOUSE, (Dec. 2, 2019), https://www.chathamhouse.org/2019/12/application-international-law-state-cyberattacks (explaining that cyber operations that cause injury or death to persons or damage or destruction of objects could amount to a use of force or armed attack under the UN Charter); *Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security*, 5–6 U.N. Doc. A/AC.290/2021/CRP.2 (Mar. 10, 2021).

121. *See Founding Member States*, *supra* note 73; Ney, *supra* note 17 (Mr. Ney's speech at Cyber Command's legal conference articulated the view that a cyber operation conducted by the U.S. or against the U.S. that has a similar impact and effect as a traditional kinetic operation, such as death, injury, and destruction would be considered a use of force); Corn, *Cyber National Security*, *supra* note 10, at 409.

122. *See* Greig, *supra* note 6 (stating that Russia has been accused of harboring and in some cases helping ransomware gangs conduct attacks on organizations across the globe); Corn & Renals, *supra* note 60, at 26–32 (hypothesizing cyber operations that could be encompassed by the DoD's Defend Forward Strategy which include the involvement of third-party states).

123. Ney, *supra* note 17; Corn, *Cyber National Security*, *supra* note 10 (noting the differences between the physical network and logical layer of cyberspace).

124. *See* Nakashima & Bennett, *supra* note 23 (explaining that Cybercom blocked REvil's website by hijacking its traffic).

that is similar to that of a traditional kinetic operation.[125] The U.S. cyber operation did not destroy REvil's infrastructure or damage it in a way that would be similar to a kinetic operation, such as physical effects that would be visible with the use of an explosive.[126] Additionally, there are no reported injuries or deaths associated with the U.S. cyber operation, as opposed to the potential injuries or deaths from a kinetic operation.[127] The access to REvil's server, cloning of their website, and redirecting of server traffic has not created lasting damage that is comparable to a kinetic attack that could cause REvil to have to rebuild or repair infrastructure in the way a building would need to be rebuilt or reconstructed after a kinetic operation.[128] Instead, REvil seemingly had full ability to regain access to its servers and reconfigure them back to their regular operations as evidenced by their voluntary decision to stop operations.[129] The servers themselves, being the subject of the cyber operation, were left physically undamaged and physically indistinguishable in their use and technical operation.[130]

The consequential damage to REvil's infrastructure by the U.S. cyber operation amounts to a disruption of the ransomware group's ability to operate their service, but not the destruction that would be consistent with a use of force.[131] Since the U.S. cyber operation does not reach the requisite threshold of a use of force under the U.S.

---

125. *See* Mangan, *supra* note 40 (revealing that several web sites linked to REvil were not operating); Nakashima & Bennett, *supra* note 23 (stating that Cybercom had cloned REvil's website, thereby obtaining the private keys to its servers); Ney, *supra* note 17 (articulating the DoD's approach to the U.N. Charter's prohibition on the use of force to cyberspace).

126. *See* Nakashima & Bennett, *supra* note 23 (revealing that a first inspection of REvil's webpage after Cybercom's actions did not turn up signs of compromise).

127. *See id.* (providing no indication or theory as to how the reported cyber operation could have been capable of creating any physical harm or injury).

128. *See id.* (detailing that Cybercom's action was not a hack or a takedown, but it deprived users of REvil from using the platform to extort victims); Ney, *supra* note 17 (explaining that a military cyber operation may constitute a use of force within the U.N. Charter if it causes physical injury or damage).

129. *See* Nakashima & Bennett, *supra* note 23 (explaining that REvil's servers had been temporarily hacked, which permitted the FBI to gain access); Turton & Mehrotra, *supra* note 28 (remarking that REvil appeared to return to their cyber activity and operations after stopping their operations for an extended period).

130. *See* Nakashima & Bennett, *supra* note 23 (reporting no facts to indicate evidence of physical damage, but evidence that the servers could still be accessed).

131. *See id.*

approach, the U.S. cyber operation is consistent and permissible under Article 2(4) of the U.N. Charter.[132]

2. The U.S. Operation Against REvil Was Not a Use of Force Even When Applying the Tallinn Manual's Factored Analysis Approach to the U.N. Charter's Article 2(4).

In applying the Tallinn Manual's eight factors of severity, immediacy, directness, invasiveness, measurability of effects, military character, state involvement, and presumptive legality[133] to the U.S. cyber operation, the U.S. cyber operation is permissible under Article 2(4) because it does not reach the threshold of a use of force.

Under the factor of severity, the Tallinn Manual takes the position that an operation that generates "mere inconvenience or irritation" will "never" qualify as a use of force.[134] The U.S. operation did not cause injury or death and resulted in temporary disruption of REvil's servers, which resulted in only inconvenience or irritation, if anything, to Russia's citizens who are members of REvil.[135] The U.S. operation more appropriately satisfies the factors of immediacy and directness due to the immediate impact of redirecting REvil's server traffic (where immediate consequences are more likely to be considered a use of force),[136] and the direct connection between the cyber operation and the immediate impact of redirecting REvil's server traffic (where the greater the cause and effect relationship, the more likely an action can

132. *See* Ney, *supra* note 17 (noting what constitutes a use of force in a military cyber operation); Corn, *Cyber National Security*, *supra* note 10, at 409 (explaining what most states agree qualifies as an unlawful use of force); U.N. Charter art. 2, ¶ 4; U.N. Charter art. 51 (qualifying that use of force under Article 2(4) is permissible when sufficiently justified under Article 51); *see* Ney, *supra* note 17 (under the application of the use of force threshold under the DoD position, a justification under Article 51 of the U.N. Charter or otherwise is unwarranted under the conclusion that the cyber operation did not arise to the level of a use of force); Corn, *Cyber National Security*, *supra* note 10, at 499; U.N. Charter art. 2 ¶ 4.

133. *See Tallinn Manual*, *supra* note 20, at 333 ¶ 9 (analyzing certain elements of cyber operation through the Tallinn Manual's eight factors).

134. *See id.*

135. *See* Nakashima & Bennett, *supra* note 23 (providing no reports or suggestions that anyone was inconvenienced by the operation); Mangan, *supra* note 40 (lacking any report of injury or death from the U.S. operation against RElive).

136. *See Tallinn Manual*, *supra* note 20, at 334 ¶ 9(b)–(c) (explaining what the immediacy and directness factor is supposed to analyze).

be characterized as a use of force).[137]

Invasiveness is described as the degree of intrusion into the subject state's cyber systems that is contrary to that state's interests.[138] In this regard, the U.S. cyber operation does not meaningfully intrude into Russian cyber systems. The U.S. operation remotely accessed REvil's servers and redirected traffic away from those servers.[139] The impact of that operation would plausibly involve using Russian information infrastructure to communicate with REvil's server, and potentially redirecting Russian internet users away from that server and to the cloned webpage.[140] While the operation likely invariably involves some level of intrusion into Russian cyber infrastructure, the intrusion and focus are directed toward non-state owned or operated servers that would be more akin to a "non-accredited system at a civilian university or small business"[141] and are therefore minimally invasive on Russia's state interests.

Measurability of effects and military character refer to quantifiable or identifiable consequences of an action and the connection between the cyber operation and military involvement.[142] The military character factor weighs in favor of a use of force due to the obvious and apparent connection between Cyber Command and the cyber operation against REvil.[143] The measurability of effects, however, weighs against a use of force. The Tallinn Manual suggests the more likely a cyber operation's consequences can be quantified, the easier its impact is to measure and therefore the more likely it may be characterized as a use of force.[144] In application to the U.S. cyber

137. *See id.*

138. *See id*. at 334 ¶ 9(d).

139. *See* Nakashima & Bennett, *supra* note 23 (writing that one of REvil's leaders saw that the site's traffic had been redirected).

140. *See generally id.* (noting that public reporting does not indicate specific methods used to disrupt REvil's servers, but it is possible that Russia's information infrastructure was utilized to support communication with the server); Greig, *supra* note 6.

141. *Tallinn Manual*, *supra* note 20, at 334–35 ¶ 9(d).

142. *See id.* at 335–36 ¶ 9(e)–(f) (explaining the two elements).

143. *See* Nakashima & Bennett, *supra* note 23 (detailing Cybercom's hijacking against REvil); Barnes, *supra* note 8 (acknowledging that the U.S. military has acted against ransomware groups, including REvil).

144. *See Tallinn Manual*, *supra* note 20, at 335–36 ¶ 9(e) (detailing the measurability of effects element).

operation, the impact is far more subjective where REvil, and not Russia's government, was the target of the operation, and the operation amounted to a temporary disruption of REvil's operations.[145]

The last two Tallinn Manual factors, state involvement and presumptive legality, refer to the level of participation of the state conducting the operation and the presumption that acts that are not prohibited under international law are permissible.[146] The connection between the cyber operation and the U.S. involvement is strong under this particular factor. In application to the U.S. cyber operation, the U.S. armed forces, under Cyber Command, are reported to have directly conducted the operation against REvil and therefore present clear and high-level state involvement in the operation.[147] In regard to presumptive legality, the operation has not expressly violated an internationally recognized prohibition per se,[148] and as a result this factor does not weigh strongly in favor of being a use of force.

Considering the weight of all eight factors suggests that a strict analysis may yield that four of the factors weigh in favor of a use of force (immediacy, directness, military character, and state involvement). However, the Tallinn Manual stresses that the factored analysis approach is intended "to identify cyber operations that are analogous to other non-kinetic or kinetic actions" that commonly would be described as a use of force,[149] as would be consistent with Rule 69's express wording.[150] The incongruent comparison of the U.S. cyber operation with the level of impact associated with a traditional kinetic operation leads to a conclusion under the factored analysis that

145. *See* Nakashima & Bennett, *supra* note 23 (noting that Cybercom's action was a temporary deprivation of use of REvil for criminals of the platform); Turton & Mehrotra, *supra* note 28 (explaining that REvil was restored after a period of being offline).

146. *See Tallinn Manual*, *supra* note 20, at 336 ¶ 9(g)–(h) (detailing the state involvement and presumptive legality factors).

147. *See* Barnes, *supra* note 8 (connecting the U.S. military to acts against ransomware groups, including REvil); Nakashima & Bennett, *supra* note 23 (explaining how a pair of operations by Cyber Command and a foreign government caused REvil to temporarily shut down).

148. *See Tallinn Manual*, *supra* note 20, at 336 ¶ 9(h) (detailing the presumptive legality factor); Nakashima & Bennett, *supra* note 23 (lacking any information of physical injury or damage caused by Cybercom's actions).

149. *Tallinn Manual*, *supra* note 20, at 333 ¶ 9.

150. *See id.* at 330 (providing the complete Rule 69).

the cyber operation was not a use of force.[151] This, in addition to the severity factor's recognition that operations resulting in inconvenience or irritation never arise to the level of a use of force[152]—and the otherwise lacking use of force characteristics of invasiveness, measurability of effects, and presumptive legality—advance the conclusion that even under the Tallinn Manual's factored analysis, the U.S. cyber operation does not constitute a use of force and is consistent with Article 2(4).

In applying the appropriate Article 2(4) standards under both the DoD position and the Tallinn Manual to the U.S. cyber operation against REvil, the cyber operation did not reach the requisite threshold of a use of force because it did not have an impact similar in effect and scope to a traditional kinetic operation that reaches the threshold of a use of force.

B. THE U.S. OPERATION AGAINST REVIL WAS NOT A PROHIBITED INTERVENTION UNDER CUSTOMARY INTERNATIONAL LAW DIRECTED TOWARDS RUSSIA BECAUSE THE OPERATION DID NOT IMPACT RUSSIA'S *DOMAINE RÉSERVÉ* AND IT WAS NOT COERCIVE.

To be permissible under international law, the U.S. operation must additionally be consistent and permissible under the customary international law obligation to refrain from prohibited interventions.[153] Specifically, a prohibited intervention is an act that requires both an impact on a state's *domaine réservé* and that the act is done in a manner that is coercive such that it subverts the victim state's ability to have autonomy.[154] To be impermissible under international law, the

151. *See id.*

152. *Id.* at 334 ¶ 9(a).

153. *See* Ney, *supra* note 17 (explaining that customary international law obligates states to follow certain behaviors and state practices); Corn, *Cyber National Security*, *supra* note 10, at 413 (stating that the principle of non-intervention is universally accepted as primary rules of international law binding on states); *Prohibition of Intervention*, *supra* note 14, at ¶ 1–2 (providing that under customary international law, a prohibited intervention obligates states to refrain from conducting activities against other states which impact their internal affairs).

154. *See Prohibition of Intervention*, *supra* note 14, at ¶ 2–4 (detailing what constitutes a prohibited intervention); *Nicar v. U.S.*, 1986 I.C.J., 14 ¶ 191 (June 27) (articulating the domaine réservé of a state as areas a state is permitted to decide freely); *see* Corn, *Cyber National Security*, *supra* note 10, at 411 (understanding

U.S. operation must have impacted an area under Russia's *domaine réservé* and it must have been coercive (the application on the prohibition on intervention would accordingly be applied to a third-party state in the event a third-party state was hosting REvil's servers that were targeted by the operation).[155]

1. The U.S. Cyber Operation Against REvil Did Not Have a Sufficient Connection to an Area of Russia's Domaine Réservé.

By utilizing private access keys to access REvil's server,[156] Cyber Command's connection with the server likely would have, at some point, utilized Russian internet infrastructure to relay Cyber Command's communication with the server (under the assumption that REvil's servers were in Russia).[157] In this instance, Cyber Command's operation could not have impacted the political, economic, or social systems of the Russian government. In redirecting REvil's server traffic, the political, economic, and social systems of the state would have been left undisturbed and under the full autonomy of the Russian government.[158]

---

domaine réservé as areas including political, economic, and social systems and foreign policy, and addressing a lack of clarity as to the scope of domaine réservé, but inference in a highly domestic matter will sufficiently touch on a state's domine réservé); *see Prohibition of Intervention*, *supra* note 14, at ¶ 3 (addressing clarity is lacking as to the scope of domaine réservé in an increasingly globalized and interdependent international community).

155. *See* Corn & Renals, *supra* note 60, at 26–32 (addressing the possibility that third-party states could be involved in hosting infrastructure that is the target of a cyber operation).

156. *See* Nakashima & Bennett, *supra* note 23 (explaining that the U.S. cyber operation utilized private access keys to access REvil's server and redirect traffic from the server to another webpage cloned by Cyber Command).

157. *See* Nakashima & Bennett, *supra* note 23 (indicating U.S. operators were able to remotely access REvil's servers that host their publicly available ransom platform); Corn & Renals, *supra* note 60, at 26–32 (emphasizing the reasonable possibility that some or most of REvil's server targeted by the U.S. operation could have been in a third-party state); *see generally Prohibition of Intervention*, *supra* note 14, at ¶ 2 (addressing that the U.S. obligation to refrain from prohibited interventions would be applied to a third-party state when they were the subject of U.S. operation).

158. *See* Nakashima & Bennett, *supra* note 23 (providing no indication that disrupting REvil's operations can be connected to the Russian State's political, economic, or social systems).

While the connection is attenuated, one could argue that any use of Russia's internet infrastructure would impact an area of Russia's *domaine réservé* because the act would implicitly be usurping Russia's internal sovereign prerogative over law enforcement and thereby act on a political[159] area reserved for the Russian government to control. Such an attenuated connection, however, remains uncompelling in the face of the fact-specific inquiry as to whether the operation acted on an area under the sole prerogative of the Russian State. [160] In this regard, the facts known about the U.S. operation would suggest that the communication with a Russian server, even when partially utilizing Russian internet infrastructure, does not fall under the sole prerogative of the Russian State when that server is connected to the global internet infrastructure and regularly engaging with external internet communications.

The Tallinn Manual articulates a consistent approach to the prohibition on interventions under Rule 66.[161] The Tallinn Manual stresses that the "key" to satisfying the *domaine réservé* element is that the state action must be designed to undermine the state's control over an area within its *domaine réservé*.[162] In this manner, the U.S. operation cannot reasonably be interpreted as meeting this standard. The U.S. cyber operation targeted REvil to disrupt its criminal ransomware operations.[163] By conducting the operation, it is infeasible to see a manner in which the operation, targeting a criminal ransomware group, was in fact designed to undermine the Russian government's ability to control its political, economic, or social systems or foreign policy.[164] With a focus on taking offensive cyber

159. *See* Nakashima & Bennett, *supra* note 23 (noting that Cyber Command's use of Russian internet infrastructure would in effect be utilized to initiate and carry out its disruption of REvil's server); *Prohibition of Intervention*, *supra* note 14, at ¶ 3; Corn, *Cyber National Security, supra* note 10, at 411.

160. *See Prohibition of Intervention*, *supra* note 14, at ¶ 3 (explaining what areas lie solely in the responsibility of the domestic affairs of a state); Corn, *Cyber National Security*, *supra* note 10, at 411 (defining domaine réservé).

161. *See Tallinn Manual*, *supra* note 20, at 312.

162. *Id.* at 315 ¶ 11.

163. *See* Nakashima & Bennett, *supra* note 23 (explaining how REvil temporarily shut down after Cybercom hijacked its site).

164. *See id.* (providing facts of the operation and its scope which indicate that the operation was designed specifically to interrupt REvil's operations); Barnes, *supra* note 8 (detailing U.S. military acts against ransomware groups, including REvil).

operation against REvil specifically, the U.S. cyber operation did not contain the requisite key to satisfying the *domaine réservé* element of a prohibited intervention under international law.[165]

2. The U.S. Operation Was Not Coercive in a Manner That Would Subvert Russia's Ability to Freely Decide in an Area Within Its Domaine Réservé.[166]

There are two well-established elements of a prohibited intervention under international law: the act must be taken against the state's *domaine réservé*, and it must be coercive enough to deny the state the ability to decide freely on a matter within its *domaine réservé*.[167] The coercive effect, in addition to the use of military force, can be any means that are otherwise coercive in restricting a state's ability to decide freely on matters within its *domaine réservé*.[168]

The U.S. cyber operation against REvil does not meet the threshold of a coercive act. The U.S. operation targeted REvil, a non-state actor,[169] and temporarily disrupted its operations by redirecting its server traffic.[170] In this sense, the U.S. operation did not apply a "forcible or dictatorial"[171] pressure on the Russian government such that its ability to follow its sovereign prerogative was limited or restricted. The U.S. operation and its reported impact did not stop the Russian government or coerce the Russian government into readily taking or refraining from taking actions that would fall under its *domaine réservé*.[172] As a result of REvil's disruption in ransomware operations, Russia's political, economic, and social systems and

165. *See* Barnes, *supra* note 8; Nakashima & Bennett, *supra* note 23 (specifying that Cybercom operations were targeted against REvil); *Prohibition of Intervention*, *supra* note 14, at ¶¶ 1, 3 (listing when an intervention and/or a use of force is prohibited).

166. *See Prohibition of Intervention*, *supra* note 14, at ¶¶ 5–6.

167. *See id.* at ¶¶ 1–2 (explaining what constitutes a prohibited intervention under international law).

168. *See id.* at ¶ 6 (explaining when the element of coercion is generally assumed); Corn, *Cyber National Security*, *supra* note 10, at 412 (defining matters that fall within a state's domaine réservé).

169. *See* Barnes, *supra* note 8 (describing REvil as its own entity that is separate from the state).

170. *See id.*

171. *Prohibition of Intervention*, *supra* note 14, at ¶ 5.

172. *See id.* at ¶ 3 (defining partially what domaine réservé entails).

foreign policy could not have been conceivably impacted or altered.

The Tallinn Manual similarly posits that a prohibited intervention must include an act of coercion.[173] The Tallinn Manual, however, goes further to say that "mere coercion does not suffice to establish" a prohibited intervention and that the majority of experts shared the view that the coercive act "must be designed" to influence the outcome in a matter reserved to a state under its *domaine réservé*.[174] As previously discussed, the U.S. cyber operation's design was seemingly separate and apart from impacting Russia's *domain réservé*.[175] In the same manner, the operation was not designed to influence the outcome of a matter reserved to the Russian government.[176] Rather, the operation's focus and impact on Revil, specifically,[177] supports the assertion that the operation was not designed to influence an outcome other than to disrupt REvil's ransomware operations.

Finding that the U.S. operation against REvil was not a prohibited intervention is further supported by other cyber operations in the international community. Most notably, the 2016 Russian interference in the U.S. presidential election[178] has spurred discussion as to whether Russia's hack into the Democratic National Committee, and the subsequent release of embarrassing information obtained in the hack during critical periods in the election cycle, was a prohibited intervention.[179] Russian inference in the U.S. election evidently had a

173. *See Tallinn Manual*, *supra* note 20, at 317 ¶ 17 (stating that a constituent element of prohibited intervention is coercion).

174. *Id.* at 317 ¶ 19 (raising the threshold of a coercive act); *see also Prohibition of Intervention*, *supra* note 14, at ¶¶ 5–6 (stating that an intervention is only prohibited if it is conducted through forcible or dictatorial means).

175. *See Prohibition of Intervention*, *supra* note 14, at ¶ 3 (determining whether an area lies solely in the responsibility of the domestic affairs of the state, thereby implicating domaine réservé).

176. *See* Barnes, *supra* note 8; Nakashima & Bennett, *supra* note 23 (relaying the effects of the Cybercom hijacking against REvil specifically).

177. *See* Nakashima & Bennett, *supra* note 23 (lacking any revealed impact from Cybercom's hijacking on any other organization or individual outside of the REvil organization).

178. *See* Nakashima & Harris, *supra* note 90 (detailing how several Russian government hackers launched an attack against Clinton's personal emails).

179. *See* Hollis, *supra* note 90 (noting that a foreign government obtaining and leaking e-mails about another country's on-going election processes is not a case violating article 2(4) but could be a violation of the recognized 'duty of non-

stronger connection to the *domaine réservé* of the U.S. political system (releasing information on internal DNC emails to influence the result of the election)[180] and as a coercive act (releasing information that embarrasses a political entity campaigning for public office to impact their public support).[181] Despite the seemingly compelling case for the election interference to be a prohibited intervention, the issue remains inconclusive due in part to both a lack of clarity in what constitutes a matter under a state's *domaine réservé*, and how coercive the act must be to qualify.[182] The reported facts of the U.S. operation against REvil demonstrate a significantly less ambiguous case.[183] Where the U.S. operation was designed and focused only on disrupting REvil's ransomware operations,[184] there is no act of coercion or impact on an area within Russia's *domaine réservé*.

A prohibited intervention under international law requires an act on the *domaine réservé* and that the act be coercive.[185] In either case,

---

intervention' in customary international law).

180. *See generally id.* (examining what international law has to say about a foreign government obtaining and leaking e-mails about another country's on-going election processes); Lewis, *supra* note 91 (arguing DNC hacks do not threaten the United States' territorial integrity, but do threaten its political independence); Nakashima & Harris, *supra* note 90 (discussing how Russian government hackers attacked email accounts and delivered trove of hacked emails to WikiLeaks).

181. *See* Hollis, *supra* note 90 (detailing domestic fallout of email leak); Lewis, *supra* note 91 (arguing hacks are part of a larger Russian effort to shape politics using misinformation, subsidies, and Internet trolls); Nakashima & Harris, *supra* note 90 (detailing how hacked emails were released on WikiLeaks in a steady stream, ensuring material embarrassing to the Clinton campaign would continue).

182. *See Prohibition on Intervention*, *supra* note 14, at ¶¶ 3 & 5 (defining domestic jurisdiction and forcible or dictatorial (coercive) means); Corn, *Nat'l Sec. Digital Age*, *supra* note 74, at 963 ("To be internationally wrongful, an intervention must first bear on what is commonly referred to as the state's 'domaine réservé' . . . the measures employed must be forcible or dictatorial, or otherwise coercive, in effect depriving the state intervened against of control over the matter in question.").

183. *See* Nakashima & Bennett, *supra* note 23 ("Cybercom's action was not a hack or takedown, but it deprived the criminals of the platform they used to extort their victims . . .").

184. *See* Barnes, *supra* note 8 (explaining Cyber Command diverted traffic around servers being used by REvil); Lyngaas, *supra* note 6 (Russia's FSB intelligence agency detained multiple people associated with REvil); Nakashima & Bennett, *supra* note 23 (stating REvil shut down after a pair of operations by U.S. Cyber Command and a foreign government targeted its servers).

185. *See Prohibition on Intervention*, *supra* note 14, at ¶ 2 (explaining intervention is wrongful when it uses methods of coercion).

under both a traditional view of the requisite factors[186] and the Tallinn Manual,[187] the U.S. operation was not a prohibited intervention because it was an act insufficiently connected to Russia's *domaine réservé* and did not have a coercive effect; therefore, the operation was permissible under international law.

C. THE U.S. OPERATION AGAINST REVIL WAS NOT AN IMPERMISSIBLE INTERFERENCE OF RUSSIA'S SOVEREIGNTY.

1. The U.S. Operation Against REvil Was Permissible Under International Law Because the Operation Was Consistent with the United States' International Obligations Regarding State Sovereignty.

The DoD takes the position that sovereignty is a principle and not a rule of international law.[188] In its decision to conduct cyber operations, the DoD finds that there is insufficient state practice to conclude that sovereignty is a rule of international law.[189]

The DoD position is supported by the law of state responsibility and the Lotus principle.[190] The law of state responsibility posits that a state violates international law only when it breaches a particular obligation

186. *See id.* ¶¶ 3–6 (conducted through forcible or dictatorial means; requires an element of coercion, or at least the threat to use forcible means).

187. *See Tallinn Manual*, *supra* note 20, at 312 (showing Rule 66 prohibits coercive intervention, including by cyber means, by one state into the internal or external affairs of another).

188. *See* Ney, *supra* note 17 ("As a threshold matter, in analyzing proposed cyber operations, DoD lawyers take into account the principle of state sovereignty."); Corn, *Cyber National Security*, *supra* note 10, at 417 ("[T]he principle of sovereignty operates as an independent rule of customary international law . . .").

189. *See* Ney, *supra* note 17 ("[T]he Department believes there is not sufficiently widespread and consistent state practice resulting from a sense of legal obligation to conclude that customary international law generally prohibits such non-consensual cyber operations in another State's territory."); Egan, *supra* note 20, at 174 ("Such widespread and perhaps nearly universal practice by states of intelligence collection abroad indicates that there is no per se prohibition on such activities under customary international law."); Corn, *Cyber National Security*, *supra* note 10, at 417 ("[T]here is insufficient evidence of either State practice or *opinio juris* to support claims that the principle of sovereignty operates as an independent rule of customary international law that regulates states' activities in cyberspace.").

190. Draft Articles, *supra* note 38, art. 8 ¶¶ 1–2; Corn, *Nat'l. Sec Digital Age*, *supra* note 108, at 967.

it owes and that obligation can be attributed to that state.[191] Separately, the Lotus principle indicates that international law is violated only when a state engages in conduct that is expressly prohibited by international law.[192]

As applied to the U.S. operation against REvil, the law of state responsibility supports the conclusion that the U.S. operation was not impermissible under international law.[193] The U.S. operation likely meets some aspects of attribution based on public acknowledgments from the DoD that the United States has taken offensive operations against ransomware groups and independent media reporting indicating that the DoD conducted the operation against REvil.[194] Assuming this attribution element of state responsibility is satisfied, there is no clear international obligation that the United States failed to uphold.[195] The operation against REvil likely interfered with Russian internal sovereignty through the inherent technical

191. *See* Draft Articles *supra* note 38, art. 8 ¶¶ 1–2 ("The attribution to the State of conduct in fact authorized by it is widely accepted in international jurisprudence.").

192. *See S.S. Lotus* 1927 P.C.I.J. ¶¶ 50–53 ("[T]he necessity of ascertaining whether or not under international law there is a principle which would have prohibited . . ." an act); The Lotus, *supra* note 113, ¶ 15 ("States have the right to do whatever is not prohibited by international law . . .").

193. *See* Corn, *Nat'l. Sec Digital Age*, *supra* note 74, at 967 ("[N]ot all state activities, whether conducted in and through cyberspace or otherwise, are regulated by international law and state responsibility is simply not implicated when states engage in acts that are unregulated by international law.").

194. *See* Nakashima & Bennett, *supra* note 23 (although leaders would not confirm specifics, REvil shut down its servers following an attack by Cybercom and a foreign government); Barnes, *supra* note 8 (the U.S. military has not directly taken responsibility for the operation against REvil but has acknowledged taking offensive cyber operations against ransomware groups within a timeframe that lines up with independent reporting attributing a cyber operation against REvil by the U.S.); Mangan et al., *supra* note 40 (National Security Council official reporters that U.S. authorities expected to act against ransomware groups soon).

195. *See* Ney, *supra* note 17 ("[T]here is not sufficiently widespread and consistent State practice resulting from a sense of legal obligation to conclude that customary international law generally prohibits such non-consensual cyber operations in another State's territory"); Corn, *Cyber National Security*, *supra* note 10, at 417 ("International law simply does not obligate other States to abstain from all nonconsensual activities within the territory of another State or that might otherwise infringe on or operate to the prejudice of that State's internal sovereignty").

characteristics of a cyber operation that required communication with REvil's infrastructure located in Russia (under the assumption the servers involved in the operation were in Russia).[196] However, this interference with Russia's internal sovereignty is not inconsistent with international obligations owed to Russia.[197] Internal sovereignty[198] does not prevent states from taking unconsented activities in the realm of a state's internal sovereignty.[199]

The common state practice of espionage is indicative of this notion.[200] States across the international system engage in espionage activities in support of their state's interests.[201] An act of espionage in another state's territory is inherently unconsented activity that violates the target's internal sovereignty.[202] Nonetheless, the international community does not regard espionage as an impermissible state practice that is a per se violation of international law.[203] While the U.S. operation against REvil is not espionage in and of itself, the operation's likely interference with Russia's internal sovereignty is similar in scope and effect to an act of espionage and thus can be

196. *See* Nakashima & Bennett, *supra* note 23 (the reported facts of the operation leave open the possibility that U.S. operators could have utilized Russian information infrastructure as part of their communication and operation with REvil's server); *see* Corn & Renals, *supra* note 60, at 26–32 (stating it is a reasonable possibility based on cyber operation hypotheticals that some or even all of REvil's server targeted by the U.S. operation could have been located in a third-party state).

197. Corn, *Cyber National Security*, *supra* note 10, at 417 ("International law simply does not obligate other States to abstain from all nonconsensual activities within the territory of another State or that might otherwise infringe on or operate to the prejudice of that State's internal sovereignty").

198. *See id.* (providing that internal sovereignty is separate and distinct from territorial integrity which is protected by Article 2(4) of the U.N. Charter).

199. *See id.* ("International law simply does not obligate other States to abstain from all nonconsensual activities within the territory of another State . . .").

200. *See id.* at 418 ("[E]spionage, an activity that is clearly prejudicial to and subject to the domestic jurisdiction of the spied-upon State.").

201. *See id.* ("States routinely engage in espionage . . . States frequently acknowledge that they do so, and often have public laws authorizing intelligence collection.").

202. *See id.* ("These activities often involve undisclosed entry into the territory of other States . . .").

203. *See id.* at 418–19 ("Since the advent of the internet, States have also engaged in espionage at an ever-increasing rate in and through cyberspace, and "like traditional espionage, there is no explicit legal prohibition" that attaches to these activities.").

viewed as an activity that is not an impermissible interference with internal sovereignty and is consistent with the law of state responsibility.[204]

In addition to the law of state responsibility, the Lotus principle adds support to the conclusion that the U.S. operation against REvil was permissible under international law.[205] As applied to the U.S. operation, the Lotus principle indicates that state actions are breaches of international law when the state conduct is expressly prohibited by international law.[206] In this regard, the Lotus principle permits the conclusion that the U.S. operation against REvil was permissible and consistent with international law since there is no express prohibition on the type of operation conducted against REvil.[207]

Alternative to the DoD position, some states take an approach akin

---

204. *See* Nakashima & Bennett, *supra* note 23 ("Cybercom's action was not a hack or takedown, but it deprived the criminals of the platform they used to extort their victims."); Corn, *Cyber National Security*, *supra* note 10, at 418–19 ("These activities often involve undisclosed entry into the territory of other States, as well as actions that alter physical and virtual conditions inside the territory to permit access to and exploitation of information.").

205. *See* The Lotus, *supra* note 113, ¶ 15 ("States have the right to do whatever is not prohibited by international law . . ."); Corn, *Nat'l. Sec Digital Age*, *supra* note 74, at 967 ("not all state activities, whether conducted in and through cyberspace or otherwise, are regulated by international law . . . This may include acts that are objectionable and even prejudicial to the targeted state, but unless they implicate a binding legal obligation, responses are confined to the realm of diplomacy and retorsions (actions that are considered "unfriendly," such as sanctions, but not unlawful).").

206. *See* The Lotus, *supra* note 113, ¶ 15 ("[W]hat is not prohibited is permitted in international law . . ."); *see* Ney, *supra* note 17 ("many States' public silence in the face of countless publicly known cyber intrusions into foreign networks precludes a conclusion that States have coalesced around a common view that there is an international prohibition against all such operations . . ."); Egan, *supra* note 20, at 174 (the U.N. Charter and the prohibition on intervention have growing recognition to their application in cyberspace); *see* Ney, *supra* note 17 (international law obligations are not readily applicable to operations that fall short of the thresholds of a prohibited use of force or a prohibited intervention); Corn, *Cyber National Security*, *supra* note 10, at 416–17 (explaining there is no explicit international law obligation that regulates cyberspace or cyber operations and their interference with internal sovereignty and there is no explicit international law obligation that regulates cyberspace or cyber operations and their interference with internal sovereignty).

207. *See* The Lotus, *supra* note 113, ¶ 15 ("States have the right to do whatever is not prohibited by international law . . .").

to the Tallinn Manual[208] that states are not permitted to conduct cyber operations that violate another state's sovereignty.[209] However, the Tallinn Manual itself concedes that "[t]he precise legal character of remote cyber operations that manifest on a State's territory is somewhat unsettled in international law."[210] The admission further complicates the impact of an interpretation of sovereignty as a rule of international law.[211] The Tallinn Manual experts reasoned that lawfulness could be assessed based on the degree of infringement of territorial integrity and interference or usurpation of inherently governmental functions.[212] The factors for considering these elements, however, are admittedly contested.[213] The imprecise and contested thresholds as to the level of interference of state sovereignty that violates international law[214] makes a determination of the permissibility of the U.S. operation against REvil under this interpretation inconclusive.

Lacking a precise threshold for a violation of sovereignty as a rule of international law as applied to cyberspace,[215] the Tallinn Manual's interpretation of sovereignty lacks compelling consideration of the permissibility of the U.S. operation against REvil. Absent opinio juris and state practice to support the notion of sovereignty as a rule of international law,[216] the DoD position supported by the law of state

208. *See* Corn, *Nat'l. Sec Digital Age*, *supra* note 74, at 969 (Netherlands endorsed the Tallinn Manual).

209. *See Tallinn Manual*, *supra* note 20, at 17 (showing a straightforward application of the Tallinn Manual's rule 4 may indicate that the U.S. operation was impermissible under this interpretation of sovereignty).

210. *Id.* at 20 note 10.

211. *See id.*; Corn, *Cyber National Security*, *supra* note 10, at 419–20 ("Again, there is simply no evidence that these activities are unregulated based on an undefined espionage exception to an existing sovereignty rule.").

212. *See Tallinn Manual*, *supra* note 20, at 20, note 10 ("The International Group of Experts assessed their lawfulness on two different bases . . .").

213. *See id.* (see discussion among the Experts in comments 11, 12, 13, 14, 16, 19); *see id.* at 21, note 13 (the importance of some factors were contested in part due to a lack of opinio juris).

214. *See id.* at 21, note 14 ("[N]o consensus could be achieved as to whether, and if so, when, a cyber operation that results in neither physical damage nor the loss of functionality amounts to a violation of sovereignty.").

215. *See id.*

216. *See* Ney, *supra* note 17 ("We recognize that there are differences of opinion among States, which suggests that State practice and opinio juris are presently not

responsibility[217] and the Lotus principle[218] provide grounding support for the conclusion that the U.S. operation against REvil was permissible under international law and consistent with U.S. obligations regarding Russia's sovereignty.[219]

IV. RECOMMENDATIONS

The growing use of cyber operations by state actors has complicated the application of international law principles made in a time absent the internet and modern technology.[220] One of the more contested areas of international law and its application to cyberspace is the role sovereignty plays in the international system.[221]

The two prevailing theories about sovereignty, that it is either a

---

settled on this issue."); Egan, *supra* note 20, at 174 ("[T]here is no absolute prohibition on such operations as a matter of international law."); *see Tallinn Manual*, *supra* note 20, at 20–21 notes 10 and 13 ("The precise legal character of remote cyber operations that manifest on a State's territory is somewhat unsettled in international law . . . no consensus could be achieved as to the precise threshold at which this is so due to the lack of expressions of opinio juris in this regard."); Corn, *Cyber National Security*, *supra* note 10, at 418–20 ("Some argue that espionage constitutes a carveout from the rule of territorial sovereignty based on long-standing State practice, but offer no evidence of opinio juris to substantiate this claim.").

217. *See* Draft Articles *supra* note 38, art. 8 ¶¶ 1–2 (considering what is attributable to state responsibility and its impact on international obligations).

218. *See* The Lotus, *supra* note 113, ¶ 15 (considering the origins of the Lotus principle).

219. *See* Ney, *supra* note 17 ("The implications of sovereignty for cyberspace are complex, and we continue to study this issue and how State practice evolves in this area, even if it does not appear that there exists a rule that all infringements on sovereignty in cyberspace necessarily involve violations of international law."); Draft Articles *supra* note 38, art. 8 ¶¶ 1–2 (attributing the actions of those directed or controlled by the state to the state); The Lotus, *supra* note 113, ¶ 15 ("States have the right to do whatever is not prohibited by international law . . .").

220. *See* Corn, *Nat'l. Sec Digital Age*, *supra* 75, at 957 ("[S]tates have yet to consider, let alone adopt any international law conventions specific to cyber operations . . . looking to the 'spirit' of existing law to adapt it to the 'present-day situation.'").

221. *See id.* at 962, 967 (explaining the theories surrounding the role of sovereignty have great implications on the way states can conduct and respond to cyber operations and can be a deciding factor in their legality, and "no issue has generated as much debate in the context of cyber operations as the question of sovereignty's normative status and application"); Corn, *Cyber National Security*, *supra* note 10, at 421 ("[S]overeignty is a principle, not a rule, and its legal consequences are not fully formed in this area.").

principle or a rule in international law, each present potential and significant outcomes in deciding the legality of cyber operations under international law.[222] The U.S. government has not taken a specific approach that is binding on the entire government as to whether it follows or abides by either perspective on sovereignty.[223] Instead, the DoD has individually articulated its perspective on the role of sovereignty and its application to cyber operations.[224]

While there are strategic advantages for the United States and other states to stay mute on the role of sovereignty and its application to cyberspace, the legal clarity achieved in taking a formal position outweighs the benefits of ambiguity in the short term and gives good reason for the United States to adopt a formal position.[225]

The current U.S. approach to sovereignty as viewed through the DoD is that sovereignty is a principle of international law, not a rule binding upon state actors that would prohibit a non-consensual cyber operation on a state's territory.[226] This perspective provides the DoD

---

222. *See* Corn, *Cyber National Security*, *supra* note 10, at 411 ("[W]hether a matter falls within the *domaine réservé* of a State is a fact-specific inquiry . . . .").

223. *See* Przemysław Roguski, *The Importance of New Statements on Sovereignty in Cyberspace by Austria, the Czech Republic and United States*, LAWFARE (May 11, 2020), https://www.justsecurity.org/70108/the-importance-of-new-statements-on-sovereignty-in-cyberspace-by-austria-the-czech-republic-and-united-states/ (DoD General Counsel's Statement on Sovereignty in Cyberspace); Corn, *Nat'l. Sec Digital Age*, *supra* note 74, at 969–70 ("Mr. Ney asserts that 'States' public silence in the face of countless publicly known cyber intrusions into foreign networks precludes a conclusion that States have coalesced around a common view that there is an international prohibition against all such operations . . . '").

224. *See* Ney, *supra* note 17 (explaining how DoD considered state sovereignty when contemplating cyber operations); *see* Roguski, *supra* note 224 (stating the departmental approach to articulating the legal significance on sovereignty leaves the U.S. open to take an official opinion).

225. *See* Corn, *Nat'l. Sec Digital Age*, *supra* note 74, at 968 (demonstrating whereas in the Lotus case, the court declined to restrict Turkey's exercise of jurisdiction absent clear evidence of an established rule of international law circumscribing its freedom to do so, where it faced a clash of external and internal sovereign interests, without such legal clarity as could be achieved through a formal position, the U.S. could be subject to suit itself or be unable to take concrete action against another state which encroaches on its sovereignty).

226. *See* Ney, *supra* note 17 (articulating the DoD stance on the applicability of international law, including sovereignty, to cyberspace, and showing the DoD's approach finds permissible cyber operations that are below the use of force and prohibited intervention thresholds though other, context specific, international

immense flexibility in its ability to respond to and conduct cyber operations internationally,[227] so long as the operation falls below the comparatively well-established thresholds of a use of force or prohibited intervention. The approach, as noted in Mr. Ney's speech, also allows the DoD to continue to employ its "defend forward" concept to engage with malicious cyber operators directly.[228] [229]

From the national security perspective of the United States, or any state actor intending to take an assertive stance against malign cyber actors, maximum flexibility is desirable in responding to and mitigating threats.[230] Consequently, an official position from the United States on sovereignty as a principle of international law would seemingly be consistent with the position of the DoD[231] and articulated strategies on responding to and protecting U.S. infrastructure from malicious cyber actors.[232]

---

obligations could or may add an additional international considerations).

227. *See* Barnes, *supra* note 8 ("In response, the government is taking a more aggressive, better coordinated approach against this threat, abandoning its previous hands-off stance."); Summary: Department of Defense Cyber Strategy 2018, *supra note* 8, at 1 (detailing the steps which the U.S. will take to counteract cyber operations in the international field).

228. *See* Ney, *supra* note 17 ("'We will defend forward to disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict.'"); Summary: Department of Defense Cyber Strategy 2018, *supra note* 8, at 1.

229. *See* Corn, *Cyber National Security*, *supra* note 10, at 421 (taking an alternative position, such that sovereignty is a rule of international law, would directly restrain the DoD from continuing to pursue its defend forward concept and from conducting cyber operations against ransomware groups like that of the one conducted against REvil).

230. *See generally* Peter Pascucci & Kurt Sanger, *Revisiting a Framework on Military Takedowns Against Cybercriminals* LAWFARE (July 2, 2021), https://www.lawfareblog.com/revisiting-framework-military-takedowns-against-cybercriminals (similar to how the U.S. government reorganized its structure and priorities to address terrorism post 9/11 more effectively, the country must be able to employ a similar response to cyber attacks).

231. *See* Ney, *supra* note 17 (articulating the DoD's stance on the applicability of international law, including sovereignty, to cyberspace).

232. *See generally* Summary Department of Defense Cyber Strategy, *supra* note 8, at 1 (since the U.S. has not taken an official position on sovereignty, the U.S. could potentially use the legal ambiguity of the role of sovereignty in international law to its advantage in dissuading malicious or malign cyber actors from carrying out cyber operations against the U.S. or U.S. interests).

Without declaring a formal stance on the role of sovereignty in cyberspace, the United States takes advantage of the DoD's legal perspective providing flexibility in their ability to respond to cyber threats, while at the same time leaving open the potential view that sovereignty is a rule of international law. The measure of this effect allows the United States to respond and conduct operations in cyberspace, while leaving the possibility that the United States may consider a cyber operation conducted against the United States as potentially violating an international legal obligation or threshold not yet articulated.[233] [234] In effect, a proposed operation against the United States would have to weigh the risk that the United States may consider the action a violation of an international obligation and respond accordingly.

A. THE UNITED STATES SHOULD TAKE AN EXPLICIT POSITION ON THE ROLE OF SOVEREIGNTY AS IT APPLIES TO CYBERSPACE.

Despite some of the advantages of reveling in the ambiguities around the role of sovereignty in cyber operations, declaring an official position on the role of sovereignty presents its own long-term advantages. By declaring an official position on sovereignty's role in cyberspace, the United States can strengthen its own legal position in the cyber operations it conducts, like the one conducted against REvil, while allowing it to take additional steps to make its position consistent with other state actors who share the same position.[235]

---

233. *See* Roguski, *supra* note 224 (showing the U.S. has yet to adopt a clear position on the matter); Corn, *Nat'l. Sec Digital Age*, *supra* note 74, at 969–70 (positing state's silence precludes the U.S. from having to adopt an official position).

234. *See* Roguski, *supra* note 224 (explaining state actors who may have to consider conducting a cyber operation against the U.S. will have to also consider the impact the operation may have on an undisclosed or articulated legal position of the U.S).

235. *See Application Of International Law To States' Conduct In Cyberspace*, https://ccdcoe.org/uploads/2018/10/UK_application-of-international-law-to-states-conduct-in-cyberspace-uk-statement.pdf, (last visited Jan. 13, 2022), [hereinafter "U.K. statement"] ("The United Kingdom does not consider that the general concept of sovereignty by itself provides a sufficient or clear basis for extrapolating a specific rule or additional prohibition for cyber conduct going beyond that of non-intervention referred to above"); Corn, *Nat'l. Sec Digital Age*, *supra* note 74, at 968 ("The UK Government's position is therefore that there is no such rule as a matter of current international law.").

B. THE UNITED STATES SHOULD PROMOTE ITS POSITION ON SOVEREIGNTY TO OTHER LIKE-MINDED NATIONS TO BUILD A CONSENSUS ON THE APPLICATION OF SOVEREIGNTY TO CYBERSPACE.

With a clarified legal position, the United States should advocate for its position with like-minded nations.[236] Outside of the United States, a growing number of state actors are developing their policy towards cyber operations and ransomware groups.[237] The United States should use their clarified position to promote their position among other international actors, especially those states that are active in cyberspace operations,[238] to come up with shared understanding and approaches to the application of international law to cyber operations. Further adoption and understanding of the U.S. position by other states could further solidify the U.S. position and establish more legal clarity[239] in future U.S. cyber operations.

C. THE UNITED STATES SHOULD ADVOCATE FOR ITS POSITION ON SOVEREIGNTY TO MULTILATERAL ORGANIZATIONS TO SHAPE STATE PRACTICE AND FORMULATE BINDING AGREEMENTS ON THE APPLICABILITY OF SOVEREIGNTY TO CYBER OPERATIONS.

In addition to promoting its explicit position on sovereignty to other like-minded states, the United States should build on any consensus made with these states to develop and propose multilateral

---

236. *See* Corn, *Nat'l. Sec Digital Age*, *supra* note 74, at 969 ("Judging from Mr. Ney's speech, the DoD, and perhaps the United States, finds clear solidarity with the U.K.'s position.").

237. *See* Greig, *supra* note 6 ("All of the countries agreed that ransomware is an 'escalating global security threat with serious economic and security consequences.' The countries reiterated that ransomware requires a 'shared response' because of how complex and global the issue is."); Gold, *supra* note 7 ("Some states . . . call for a ban on the development and use of OCCs by states . . . By contrast, Western countries . . . advocate for acknowledging and speaking transparently about OCCs.").

238. *See* Cyber Operations Tracker, *supra* note 7 ("Since 2005, thirty-four countries are suspected of sponsoring cyber operations.")

239. *See* Egan, *supra* note 20, at 174 ("The United States is deeply respectful of other States' sovereign authority to prescribe laws governing activities in their territory."); *see Tallinn Manual*, *supra* note 20, at 20, note 13 ("The International Group of Experts cautioned that State practice based on a sense of legal obligation is needed to fully clarify this issue . . .").

frameworks through existing international organizations. In advocating for its position with a coalition of other states, the United States can improve its legal position in cyber operations, while also establishing international standards that other states can choose to recognize,[240] adding clarity and better understanding to international law principles and their application to cyber operations.[241] Ultimately, by advocating for its approach to international law and its application to cyber operations the United States can help shape state practice,[242] even in the absence of a binding resolution or treaty on the application of international law to cyber operations.

V. CONCLUSION

The increase in the use of ransomware by cyber-criminal groups has accelerated state involvement in protecting their critical infrastructure and economies.[243] Due to the inherent international nature of cyber

240. *See* Corn, *Nat'l. Sec Digital Age*, *supra* note 74, at 957 ("states have yet to consider, let alone adopt any international law conventions specific to cyber operations").

241. *See* Ney, *supra* note 17 ("DoD lawyers also advise on how a proposed cyber operation may implicate U.S. efforts to promote certain policy norms for responsible State behavior in cyberspace, such as the norm relating to activities targeting critical infrastructure."); Egan, *supra* note 20, at 174 ("Precisely when a non-consensual cyber operation violates the sovereignty of another State is a question lawyers within the U.S. government continue to study carefully . . ."); U.K. statement, *supra* note 235 ("The United Kingdom recalls that any prohibition on the activities of States whether in relation to cyberspace or other matters, must be clearly established either in customary international law or in a treaty binding upon the States concerned."); *Tallinn Manual*, *supra* note 20, at 20 note 10 ("The precise legal character of remote cyber operations that manifest on a State's territory is somewhat unsettled in international law."); *see Corn, Nat'l. Sec Digital Age*, *supra* note 74, at 957 (stating there is currently no specific international law or treaty that regulates cyber operations; however, a coalition of states that share the U.S. position could be influential in creating recognized frameworks on the application of international law in cyberspace and could support binding resolutions or persuasive authorities on the application of international law).

242. *Opinio juris (international law)*, CORNELL LEGAL INFO. INST., https://www.law.cornell.edu/wex/opinio_juris_(international_law), (last visited Mar. 5, 2022) ("Opinio juris denotes a subjective obligation, a sense on behalf of a state that it is bound to the law in question.").

243. *See generally* Summary Department of Defense Cyber Strategy, *supra* note 8, at 1 ("Competitors deterred from engaging the United States and our allies in an armed conflict are using cyberspace operations to steal our technology, disrupt our government and commerce, challenge our democratic processes, and threaten our

operations, a state conducting a cyber operation against a ransomware group will need to consider the implications of international law.[244] International law has been found to apply to cyberspace, and thus to cyber operations, through treaties, state recognition, and state practice.[245]

After applying the applicable and relevant international law principles of a prohibited use of force under Article 2(4) of the U.N. Charter, the prohibition on intervention under customary international law, and the principle of sovereignty to the U.S. cyber operation against REvil, the U.S. operation was permissible under international law.

However, the United States can solidify its legal position by clarifying its view of the role of sovereignty in the international system in relation to cyber operations.[246] In addition to clarifying its role, the United States should promote and reinforce sovereignty's position in

---

critical infrastructure.").

244. *See* Ney, *supra* note 17 (affirming that the DoD analyzed cyber operations "in light of the domestic and international legal considerations . . ."); Egan, *supra* note 20, at 174 ("In certain circumstances, one State's non-consensual cyber operation in another State's territory could violate international law . . .").

245. *See Consensus On The Application of Rule of Law and U.N. Charter to Make Cyberspace Safe*, U.N. (Nov. 13, 2018) https://www.un.org/sustainabledevelopment/blog/2018/11/consensus-on-the-application-of-rule-of-law-and-un-charter-to-make-cyberspace-safe ("Tremendous progress has been made internationally in accepting that international law and the UN Charter apply in cyberspace."); U.K. Statement, *supra* note 235 ("The United Kingdom does not consider that the general concept of sovereignty by itself provides a sufficient or clear basis for extrapolating a specific rule or additional prohibition for cyber conduct going beyond that of non-intervention referred to above. At the same time, the United Kingdom notes that differing viewpoints on such issues should not prevent States from assessing whether particular situations amount to internationally wrongful acts and arriving at common conclusions on such matters."); *Working Group*, *supra* note 120, at 5–6 ("States reaffirmed that international law, and in particular the Charter of the United Nations, is applicable and essential to maintaining peace and stability and promoting an open, secure, stable, accessible and peaceful ICT environment.").

246. *See* Ney, *supra* note 17 (articulating the DoD's stance on the applicability of international law, including sovereignty, to cyberspace); Egan, *supra* note 20, at 174 ("Precisely when a non-consensual cyber operation violates the sovereignty of another State is a question lawyers within the U.S. government continue to study carefully, and it is one that ultimately will be resolved through the practice and opinio juris of States.").

the international community among like-minded states[247] that similarly engage in cyber operations. By taking a clear position and engaging with international partners, the United States can help shape consistent and understandable frameworks when applying international law to cyberspace.

247. *See* Corn, *Nat'l. Sec Digital Age*, *supra* note 74, at 969 (alluding that the U.S. position could relate to the U.K.'s position on sovereignty as a principle).