INTERNATIONAL LAW STUDIES

Published Since 1895

The Strategic Use of Ransomware Operations as a Method of Warfare

Jeffrey Biller

100 INT'L L. STUD. 483 (2023)

Volume 100

2023

Published by the Stockton Center for International Law

ISSN 2375-2831

The Strategic Use of Ransomware Operations as a Method of Warfare

*Jeffrey Biller**

CONTENTS

* Professor, United States Air Force Academy.

The thoughts and opinions expressed are those of the author and not necessarily those of the U.S. government, the U.S. Departments of the Navy or Air Force, or the U.S. Naval War College or Air Force Academy.

I. INTRODUCTION

Grand military strategists regularly emphasize that, although the nature of war does not change, the character of war is constantly evolving. General Mark Milley, the Chairman of the Joint Chiefs of Staff, has further stated that the character of warfare is in the midst of fundamental change.[1] As such, evolving technologies should constantly be evaluated for their potential use in warfare, including legal, policy, and ethical limitations. There is no shortage of projects, articles, and books examining the use of cyber capabilities in armed conflicts. These texts focus on threshold legal questions, such as when the use of cyber capabilities constitutes a use of force or hostilities, as well as the use of cyber to deliver traditional military effects on the battlefield. A frequent topic of discussion includes the legal protections for civilian data during armed conflicts.[2] Given that States will always seek to leverage new technologies to achieve advantages in the battlespace, it would be dangerously short-sighted not to consider all potential uses of cyber capabilities in armed conflicts, including ransomware as a method of warfare.

The use of ransomware in armed conflicts has increased urgency with Russia's invasion of Ukraine. As of the writing of this article, no NATO country has become a party to the conflict. However, the provision of arms and other avenues of support to Ukraine by several nations, including the United States, has raised difficult questions of neutrality.[3] Russia has also declared that sanctions imposed by the United States and other members of the international community "are like a declaration of war."[4] Issues of neutrality are outside the scope of this article. However, there is an increased possibility that Russia will employ cyber capabilities, including ransomware, against those States Russia sees as supporting Ukraine in the armed conflict. More to the point of this article, Russia could also use ransomware against Ukraine to get the Ukrainian government to capitulate to Russian demands.

---

1. John Grady & Sam LaGrone, *CJCS Milley: Character of War in Midst of Fundamental Change*, USNI NEWS (Dec. 4, 2020), https://news.usni.org/2020/12/04/cjcs-milley-character-of-war-in-midst-of-fundamental-change.

2. *See, e.g.*, Robin Geiß & Henning Lahmann, *Protection of Data in Armed Conflict*, 97 INTERNATIONAL LAW STUDIES 556 (2021).

3. Wolff Heinstchel von Heinegg, *Neutrality in the War Against Ukraine*, ARTICLES OF WAR (Mar. 1, 2022), https://lieber.westpoint.edu/neutrality-in-the-war-against-ukraine/.

4. Timothy Bella, *Putin Likens Sanctions to a "Declaration of War," Says Invasion Pushback Risks Future of Ukrainian Statehood*, WASHINGTON POST (Mar. 5, 2022), https://www.washingtonpost.com/world/2022/03/05/putin-russia-ukraine-statehood-sanctions/.

Ransomware differs from most cyber operations in that its nature is coercive rather than exploitative.[5] It creates reversible conditions to force an adversary to give-in to pre-established demands. Most cyber operations are exploitive in that the only intended action is on the part of the aggressor. Most malicious cyber operations are designed to achieve a set of effects regardless of how the adversary responds. While they can be quite effective in achieving favorable outcomes such as intelligence gathering or disruption of command and control, they are not generally designed to force a change of behavior on the part of an adversary.[6] As a coercive tool, however, ransomware could be used effectively in armed conflicts to force an opponent to accept a set of demands. Although its use could be limited to military objects where the law is relatively permissive, States might also use ransomware against a broader range of targets. In particular, civilian targets of great everyday utility to the public might pressure a government to resolve a conflict. Given the lack of clarity over the status of civilian data in armed conflicts generally, and the unexamined analysis of ransomware use against civilian targets, the time is ripe to examine the legal limitations on the use of ransomware under international humanitarian law (IHL).

This article examines the potential use and legal limitations of ransomware, defined here as the temporary encryption of data until some pre-condition is met to release the encryption, to achieve strategic effects in armed conflicts. It does not broach the thorny issues of peacetime sovereignty, illegal uses of force under the United Nations Charter, whether non-violent cyber effects can constitute hostilities for purposes of conflict classification, or the use of ransomware in non-international armed conflicts. Instead, it is limited to a State's potential use of ransomware against another State, where both are parties to an existing international armed conflict. This article is also limited to an examination of international law. The domestic laws and policies governing the employment of offensive cyberspace capabilities are not covered. Ultimately, this author finds that IHL does not currently prohibit most uses of ransomware against non-military related targets in armed conflicts. Fundamentally, data neither forms a tangible object nor constitutes

5. *See generally* MICHAEL P. FISCHERKELLER ET AL., CYBER PERSISTENCE THEORY: REDEFINING NATIONAL SECURITY IN CYBERSPACE (2022).

6. There are, of course, exceptions to this statement. For example, North Korea was somewhat successful in preventing the release of the movie "The Interview" by launching malicious, non-reversible, cyber operations against Sony Pictures. Alex Altman & Alex Fitzpatrick, *Everything We Know About Sony, The Interview and North Korea*, TIME (Dec. 17, 2014), https://time.com/3639275/the-interview-sony-hack-north-korea/.

real or personal property. Data is information and, therefore, must be considered in, not isolated from, the context of its use. While the encryption of data may be a legal violation when it inhibits the functionality of specific protected categories, civilian data cannot be said to have per se protection. This argument is strengthened when considered in the context of temporary encryption, as opposed to permanent corruption. Recognizing the potential dangers presented by the use of ransomware in armed conflicts, this article identifies primary legal and ethical questions that States must resolve to protect non-military related data from ransomware operations in armed conflicts.

II. CYBERSPACE AND INTERNATIONAL HUMANITARIAN LAW

State pronouncements of *opinio juris* and an intense stretch of work by academics have driven significant advancement in the legal understanding of IHL applicability to cyber operations. Perhaps the most notable effort is the *Tallinn Manual* project, now working toward its third edition.[7] Despite these efforts, cyber remains a topic of great debate with myriad unresolved questions.[8] Recognizing this ambiguity, States and international organizations are beginning to make more detailed statements about their positions.[9] However, these efforts have been tentative at best as States struggle to formulate their strategies for cyber operations in peacetime and armed conflicts. Undoubtedly, the use of cyber operations by States in armed conflicts is already a reality. It will accelerate as the technology becomes available to more States and they refine the doctrine surrounding its use.[10] Many of these cyber operations will constitute traditional military activities; for example, an attempt

7. TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS (Michael N. Schmitt gen. ed., 2017).

8. *See generally* Laurent Gisel et al., *Twenty Years On: International Humanitarian Law and the Protection of Civilians Against the Effects of Cyber Operations During Armed Conflicts*, 102 INTERNATIONAL REVIEW OF THE RED CROSS 287 (2020).

9. For a recent overview of States' positions, *see* Przemysław Roguski, *Application of International Law to Cyber Operations: A Comparative Analysis of States' Views*, HAGUE PROGRAM FOR CYBER NORMS POLICY BRIEF (Mar. 2020), https://ruj.uj.edu.pl/xmlui/bitstream/handle/item/153989/roguski_application_of_international_law_to_cyber_operations_2020.pdf. *See also* Int'l Comm. of the Red Cross, Position Paper: International Humanitarian Law and Cyber Operations During Armed Conflicts (Nov. 28, 2019), http://www.icrc.org/en/document/international-humanitarian-law-and-cyber-operations-during-armed-conflicts.

10. *See* Statement of General Paul M. Nakasone, Commander, United States Cyber Command, before the Senate Committee on Armed Services (Feb. 14, 2019), https://www.armed-services.senate.gov/imo/media/doc/Nakasone_02-14-19.pdf.

to disable integrated air defense systems or military command and control networks. Cyber operations have already seen extensive use in traditional information warfare methods such as propaganda and military deception.[11]

While using cyber capabilities against traditional military objectives is worthy of study, new and innovative uses of cyber capabilities in armed conflicts against other categories of targets will undoubtedly advance in the coming years. Because many of these uses may potentially involve civilian targets, the legal implications of all potential uses should be explored. Among these possible methods of cyber operations, ransomware use in armed conflicts is a particularly fascinating topic as it encapsulates many of the current debate areas. Issues such as when cyber operations qualify as an "attack," how to analyze cyber operations that fail to qualify as an attack, if and when data might qualify as an object, and what categories of civilian data should receive special protections must all be considered in the analysis. This article begins by exploring the basics of ransomware and providing examples of previous uses. Next, it explores fundamental issues of IHL application, such as targeting law and special protections, cyber operations generally, and ransomware in particular. Finally, it concludes with a discussion of potential normative limitations on certain potential targets of ransomware operations.

III. RANSOMWARE—WHAT IS IT?

The concept of ransomware is quite simple and elegant in its way. At its simplest, ransomware is a type of malicious software, or malware, designed to deny access to a computer system or resident data until a ransom is paid.[12] Ransomware frequently spreads through phishing emails or a target user unknowingly visiting an infected website.[13] Some ransomware operations have also utilized worms, permitting malicious code to transmit from computer to computer without human interaction. Although ransomware operations continue to proliferate and increase in sophistication, this basic methodology continues to be effective. States have struggled to find policy solutions to deter ransomware operations, but the problem set is quite resilient. Malicious

11. *See, e.g.*, Christian Perez & Anjana Nair, *Information Warfare in Russia's War in Ukraine*, FOREIGN POLICY (Aug. 22, 2022), https://foreignpolicy.com/2022/08/22/information-warfare-in-russias-war-in-ukraine/.

12. Cybersecurity & Infrastructure Security Agency, *Ransomware Guide* (Sept. 2020), https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf.

13. *Id.*

operators continue to add new twists to their methodology, from deleting backup systems simultaneously to encrypting the primary data set.[14] Malicious actors then demand ransom in exchange for decryption.[15] The explosion of cryptocurrencies also fuels the rise of ransomware operators, providing relatively secure and anonymous ways to transfer payment funds.[16]

Organizations with essential data stored on a computer or network, particularly those with clients or customers who need regular access to that data, are at risk. However, in recent years the use of ransomware against governmental organizations, particularly at state, local, tribal, and territorial levels, as well as critical infrastructure entities, has been increasingly prevalent. In 2020, the U.S. Federal Trade Commission found: "industry sources report a major surge in the number of ransomware attacks in 2020. . . . As ransomware has grown into a serious 'business,' attackers have become increasingly sophisticated."[17] That trend shows no signs of slowing down. Particularly appealing targets include organizations holding large volumes of privacy data, including hospitals. For example, malicious operators hit Universal Health Services with a ransomware operation that caused medical records, labs, and pharmacies to go offline and required ambulances to be diverted.[18]

Although large corporations with the capability to pay ransoms ranging up to U.S. $10 to 30 million would appear to be the obvious targets, even school districts have found themselves subject to extortion from malicious operators through ransomware operations.[19] What makes these targets so effective is that these organizations are essential to most people's everyday

14. Lawrence Abrams, *Zenis Ransomware Encrypts Your Data & Deletes Your Backups*, BLEEPINGCOMPUTER (Mar. 16, 2018), https://www.bleepingcomputer.com/news/security/zenis-ransomware-encrypts-your-data-and-deletes-your-backups/.

15. *Id.*

16. Law enforcement, however, seems to have made great advances in tracking the transfer of cryptocurrencies. *See, e.g.*, Brett Wolf, *US Law Enforcers Partner with Cryptocurrency Tracking Firm to Fight Financial Crime*, THOMSON REUTERS (Dec. 23, 2020), https://www.thomsonreuters.com/en-us/posts/investigation-fraud-and-risk/cryptocurrency-financial-crime/.

17. Ben Rossen, *Ransomware Prevention: An Update for Businesses*, FEDERAL TRADE COMMISSION (Dec. 11, 2020), https://www.ftc.gov/business-guidance/blog/2020/12/ransomware-prevention-update-businesses.

18. Robert McMillan & Jenny Strasburg, *Mounting Ransomware Attacks Morph Into a Deadly Concern*, WALL STREET JOURNAL (Sept. 30, 2020), https://www.wsj.com/articles/mounting-ransomware-attacks-morph-into-a-deadly-concern-11601483945.

19. Tawnell D. Hobbs, *Schools Struggling to Stay Open Get Hit by Ransomware Attacks*, WALL STREET JOURNAL (Nov. 13, 2020), https://www.wsj.com/articles/my-information-is-out-there-hackers-escalate-ransomware-attacks-on-schools-11605279160.

lives. Without access to user data, critical functions of society grind to a halt. Thus, there is often intense social and political pressure to pay the ransom and release the data. The pressure is potentially similar when practiced by a State as part of an armed conflict. Another factor advancing ransomware proliferation is the lack of a need for specific, defined targets. Instead, operators can continually scan for soft targets containing easily exploitable vulnerabilities, bypassing hardened and secure targets.

Among the most notable ransomware operations was the global operation known as WannaCry. The operation began in May 2017 and affected more than 150 countries.[20] WannaCry operated like most ransomware operations, encrypting the data on your computer, then displaying a demand for payment, typically in hard-to-track Bitcoin, in return for the ability to decrypt your data.[21] WannaCry was notable for its scale and some high-visibility targets hit by the operation, such as Britain's National Health Service and Boeing. It was also noteworthy because it appears to have utilized a National Security Agency tool, EternalBlue, which hackers had acquired.[22] Although the Department of Justice ultimately indicted a North Korean national, Park Jin Hyok, for the crime, the effects of the operation were felt for years.[23]

Another high-profile ransomware operation was the Petya malware, first discovered in March 2016. Several variants of Petya were ultimately discovered, including the even more harmful NotPetya emerging in June 2017. NotPetya was notable for using the same EternalBlue exploit found in WannaCry and because it could encrypt the master boot record, rendering the entire infected computer unusable.[24] Security experts largely believe that Russian-backed hacking groups developed Petya and its variants for initial use against Ukraine as part of the armed conflict beginning in 2014 and as a

20. Ian Sherr, *WannaCry Ransomware: Everything You Need to Know*, CNET (May 19, 2017), https://www.cnet.com/news/wannacry-wannacrypt-uiwix-ransomware-everything-you-need-to-know/.

21. *Id.*

22. Danny Palmer, *WannaCry Ransomware Is Still Infecting PCs—And Some Victims Are Still Trying to Pay the Ransom*, ZDNET (Sept. 20, 2019), https://www.zdnet.com/article/wannacry-ransomware-is-still-infecting-pcs-and-some-victims-are-still-trying-to-pay-the-ransom/.

23. Charlie Osborne, *North Korea Claims Hacker Responsible for WannaCry Outbreak Does Not Exist*, ZDNET (Sept. 14, 2018), https://www.zdnet.com/article/north-korea-claims-hacker-responsible-for-sony-breach-does-not-exist/.

24. Cybersecurity & Infrastructure Security Agency, Alert (TA17-181A) Petya Ransomware (Feb. 15, 2018), https://us-cert.cisa.gov/ncas/alerts/TA17-181A.

testing ground for Russian cyber capabilities.[25] However, NotPetya infections ultimately spread worldwide, impacting the finance, transportation, and healthcare sectors, among others.[26] The other notable feature of NotPetya was that while it was quite harmful, it proved largely unsuccessful in extorting money, which may have been intentional.[27]

Perhaps most relevant to this study is using various ransomware capabilities to extort money from governments, particularly those that have targeted local government agencies providing vital services to local populations. Prime examples include the ransomware operations against the cities of Greenville, North Carolina, and Baltimore, Maryland, in May of 2017. These operations used a ransomware capability known as "RobbinHood" to gain access to and subsequently encrypt city administrative accounts.[28] Local governments are prime targets because they often have poor network security due to inadequate funding, and the political pressure to restore affected local services is significant. For example, it brought the entire real estate market to a complete halt in Baltimore.[29]

Ransomware is undoubtedly one of the most effective existing criminal methods, cyber or otherwise. This is true both for private actors and States such as North Korea.[30] What, however, would be the advantage of using ransomware in an armed conflict? Ransomware, in its essentials, is nothing more than encrypting another user's data and preventing its use until you provide them with the decryption key. The benefit of encrypting military-related data during an armed conflict is straightforward and non-controver-

25. Andy Greenberg, *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*, WIRED (Aug. 22, 2018), https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

26. Alert (TA17-181A) Petya Ransomware, *supra* note 24.

27. *Cyber-Attack Was About Data and Not Money, Say Experts*, BBC NEWS (June 29, 2017), https://www.bbc.com/news/technology-40442578.

28. Ian Duncan & Christine Zhang, *Analysis of Ransomware Used in Baltimore Attack Indicates Hackers Needed "Unfettered Access" to City Computers*, BALTIMORE SUN (May 17, 2019), https://www.baltimoresun.com/politics/bs-md-ci-ransomware-attack-20190517-story.html.

29. *Id.*

30. U.S. Dep't of the Treasury, Press Release: Treasury Sanctions North Korean State-Sponsored Malicious Cyber Groups (Sept. 13, 2019), https://home.treasury.gov/news/press-releases/sm774.

sial. Take the hypothetical example of one party to an armed conflict encrypting its adversary's targeting database.[31] The military advantage of such an action is quite clear. Similarly, a State might use ransomware against certain war-supporting functions, such as a State's defense industrial base, with the data encrypted until the end of a conflict. Although in most situations there would be little reason not to simply delete the data, it is possible that encryption might make more sense. Possible examples include a desire for the adversary to become an ally at the end of the conflict and where there is a need for the vanquished State to continue as a balancing regional power.

The better, or at least more interesting, legal question is what would be the advantage of using ransomware against non-military objectives during an armed conflict?[32] The answer is to apply non-violent methods of reducing an adversary's public support for the conflict and pressuring that State into negotiations to end the conflict. This method echoes the "strategic bombing" of the early- to mid-twentieth-century campaigns that largely proved a failure in breaking civilian morale and support for their governments. During the combined bombing offensive in World War II by the American 8th Air Force and Royal Air Force Bomber Command, British leaders argued for a goal of "de-housing" large portions of the German population to "break the spirit of the people."[33] Whether that was an official goal of the combined bombing offensive or not, it never broke German civilian morale.

If the use of air power to break the public will be proved largely ineffective, why would a State resurrect this strategy through the strategic use of ransomware? There are several possibilities. First, it would allow a militarily weaker party to a conflict to demonstrate action to its public audience. This strategy has been cited as a reason for the use of strategic bombing as well.[34]

---

31. *See, e.g.,* Julian E. Barnes, *U.S. Cyberattack Hurt Iran's Ability to Target Oil Tankers, Officials Say*, NEW YORK TIMES (Aug. 28, 2019), https://www.nytimes.com/2019/08/28/us/politics/us-iran-cyber-attack.html.

32. As will be discussed in greater depth below, military objectives are defined by the International Committee of the Red Cross as "those objects which by their nature, location, purpose or use make an effective contribution to military action and whose partial or total destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage." 1 CUSTOMARY INTERNATIONAL HUMANITARIAN LAW r. 8 (Jean-Marie Henckaerts & Louise Doswald Beck eds., 2005).

33. John T. Correll, *The Allied Rift on Strategic Bombing*, AIR FORCE MAGAZINE (May 4, 2022), https://www.airforcemag.com/article/the-allied-rift-on-strategic-bombing/.

34. Ian Buruma, *Why "Strategic" Bombing Doesn't Seem to Work*, THE GLOBE AND MAIL (Aug. 6, 2014), https://www.theglobeandmail.com/opinion/why-strategic-bombing-doesnt-seem-to-work/article19928220/.

Second, it could be theorized that if the public knew the adverse effects of the ransomware could be reversed relatively quickly, as opposed to the time-intensive process of rebuilding a bombed-out city, there might be a greater likelihood of the public placing pressure on their government to end the conflict quickly. Cyber operations can cause inconvenience to the public without the graphic images of death and destruction that follow bombing campaigns and that generate intense feelings of resentment towards the adversary. Finally, unlike intentionally targeting civilians with violence, it may be legal under international law. This article analyzes this final question, addressing the potential arguments against legality. These arguments include violations of the rule of distinction, special protections provided to certain potential targets, the question of targeting economic or war-sustaining targets, and non-legal normative arguments. Each of these will be addressed below in turn.

IV. THE RULE OF DISTINCTION

The general application of principles of IHL to cyber is not generally controversial. For example, the 2015 report of the United Nations Group of Governmental Experts in the Field of Information and Telecommunications in the Context of International Security (hereinafter UN GGE on Cyber) affirmed the application of cyber operations to "the established international legal principles, including, where applicable, the principles of humanity, necessity, proportionality and distinction."[35] However, the specific application of the actual rules to cyber operations has proven more difficult.

Among these rules, the first and most obvious argument against using ransomware against civilians in an armed conflict is the rule of distinction. Distinction is considered a "cardinal" principle of international humanitarian law.[36] Promulgated initially in the 1868 St. Petersburg Declaration[37] and expanded upon in the 1899 and 1907 Hague Regulations,[38] it was codified in

35. *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, U.N. Doc. A/70/174, ¶¶ 24, 28(d) (July 22, 2015).

36. Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, ¶ 78 (July 8).

37. Declaration Renouncing the Use, in Time of War, of Explosive Projectiles Under 400 Grammes Weight, pmbl. ¶ 2, Dec. 11, 1868, 138 Consol. T.S. 297, 18 MARTENS NOUVEAU RECUEIL (ser. 1) 474.

38. Convention No. II with Respect to the Laws and Customs of War on Land, with annex of regulations arts. 22, 29, 32, July 29, 1899, 32 Stat. 1803, T.S. No. 403; Regulations

Additional Protocol I to the Geneva Conventions (AP I).[39] The rule of distinction protects civilians and civilian objects from attack by stating that violent force may only be directed against combatants and military objectives. Protection of civilian objects finds its most unambiguous expression in AP I, Article 52(1), requiring that "[c]ivilian objects shall not be the object of attack or reprisals."[40]

Civilian objects are quite simply those objects that do not meet the definition of a military objective: "those objects which by their nature, location, purpose or use make an effective contribution to military action and whose partial or total destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage."[41] Thus, previously civilian objects, such as vehicles, bridges, or buildings, can become military objectives during an armed conflict if they meet the definition above. However, this categorization applies only to objects. Given this article's focus on ransomware operations against data, we must first examine whether data has the potential to qualify as a civilian object.

A. Data as an Object

Information systems can be broadly broken into two categories: physical hardware and the data resident therein. Although data can be broken out into many categories depending on the question being asked, one helpful method for a legal analysis is to break it into operational and content-level data. Broadly speaking, operational data generally enables the functionality of an information system and specific applications on that system. Content-level data is that which is fed into the system for storage or analysis. Some scholars have argued that these different types of data should receive different levels of protection under IHL.[42] At a basic level, this distinction makes sense. If operational-level data is corrupted or rendered useless, then the system as a whole or the particular application will cease to function for its

---

Respecting the Laws and Customs of War on Land art. 22, annexed to Convention No. IV Respecting the Laws and Customs of War on Land, Oct. 18, 1907, 36 Stat. 2277, T.S. No. 539.

39. Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts arts. 48, 51, 52, June 8, 1977, 1125 U.N.T.S. 3 [hereinafter AP I].

40. *Id.* art. 52(1).

41. CUSTOMARY INTERNATIONAL HUMANITARIAN LAW r. 8, *supra* note 32.

42. *See, e.g.*, Heather H. Dinniss, *The Nature of Objects: Targeting Networks and the Challenge of Defining Cyber Military Objectives*, 48 ISRAEL LAW REVIEW 39, 41 (2015).

intended purpose. However, the rendering useless of content-level data theoretically only affects the access to, or analysis of, that particular data set. The system or application may otherwise continue to function as intended. However, this argument presupposes that any form of digital data might qualify as an object and potentially receive legal protections as a civilian object. Whether data constitutes an object is a core question of debate regarding the applicability of IHL to the cyber domain and must be examined in depth.[43]

Given the above definitions related to the rule of distinction, if the target of an operation does not qualify as a person or object, then the rule of distinction would fail to apply. The argument against data being considered an object relies on the traditional IHL understanding of an object as "something that is visible and tangible."[44] Because digital data (without a graphical user interface and a physical piece of hardware such as a monitor) can neither be seen nor touched, there is a strong argument that it fails to meet that traditional understanding. The counterargument takes a more flexible approach to the meaning of an object and looks to the general rule of treaty interpretation in the Vienna Convention on the Law of Treaties (VCLT). Article 31(1) of the VCLT states that "[a] treaty shall be interpreted in good faith in accordance with the ordinary meaning to be given to the terms of the treaty in their context and in the light of its object and purpose."[45] This line of logic has led some scholars and governments to argue that in the digital age, the object and purpose of IHL are best met when the definition of a military objective includes digital objects: data.[46] Indeed, modern armed conflicts will almost certainly have a cyber component. However, expanding the definition

43. This question has been explored in depth by several prominent scholars as well as the International Group of Experts (IGE) participating in the *Tallinn Manual* project. The majority of the IGE found "that the law of armed conflict notion of 'object' is not to be interpreted as including data, at least in the current state of the law." TALLINN MANUAL 2.0, *supra* note 7, at 437. However, several prominent scholars disagree with this interpretation and believe a present-day understanding of objects should include electronic data. *See, e.g.*, Dinniss, *supra* note 42; Kubo Mačák, *Military Objectives 2.0: The Case for Interpreting Computer Data as Objects Under International Humanitarian Law*, 48 ISRAEL LAW REVIEW 55 (2015); Michael N. Schmitt, *The Notion of "Objects" During Cyber Operations: A Riposte in Defence of Interpretive Precision*, 48 ISRAEL LAW REVIEW 81 (2015).

44. COMMENTARY ON THE ADDITIONAL PROTOCOLS OF 8 JUNE 1977 TO THE GENEVA CONVENTIONS OF 12 AUGUST 1949, ¶ 2008 (Yves Sandoz, Christophe Swinarski & Bruno Zimmermann eds., 1987).

45. Vienna Convention on the Law of Treaties, May 23, 1969, 1155 U.N.T.S. 331.

46. *See* discussion *supra*, note 43.

of an object to include non-visible and non-tangible items is a highly consequential change in the law. It should only come about through one of the recognized processes for creating international law: treaties and customary international law. These questions may be answered if States enter into a treaty regime governing the use of cyber capabilities in armed conflicts. Until then, we must look to customary international law for such a revision of the law.

Customary international law emerges over time through a combination of State practice and *opinio juris*, which is a State's belief that it is engaging in, or refraining from, an action out of legal obligation.[47] Although expressions of *opinio juris* related to cyber operations in armed conflicts have been limited, the existing statements regarding whether electronic data may constitute an object are inconclusive.[48] France, for example, finds that "[a]lthough intangible, . . . civilian content data may be deemed protected objects" and that "special protection afforded to certain objects extends to systems and the data that enable them to operate."[49] This article addresses those "special protections" below. Nevertheless, it is noted now that special protections do not depend on qualification as an object but are predominantly focused on functionality. On the other hand, Israel holds that "under the law of armed conflict, as it currently stands, only tangible things can constitute objects."[50]

At the current time, it is this author's opinion that incorporating electronic data into the definition of an object would be a significant departure from the original meaning of an object under both treaty and customary international law. Many of the most prominent State actors in the cyber domain, including the United States, the United Kingdom, China, and Russia, have not yet specifically addressed the question of data qualifying as an object. Should a significant number of States adopt a position firmly declaring that data constitutes an object for purposes of IHL, that could change in the

47. Statute of the International Court of Justice art. 38(1)(b), June 26, 1945, 59 Stat. 1031.

48. For an in-depth discussion of *opinio juris* in the cyber domain, *see* Michael N. Schmitt & Sean Watts, *The Decline of International Humanitarian Law Opinio Juris and the Law of Cyber Warfare*, 50 TEXAS INTERNATIONAL LAW JOURNAL 189 (2015).

49. Paper Shared by France with the Open-Ended Working Group Established by Resolution 75/240, at 15 (2021), https://documents.unoda.org/wp-content/uploads/2021/12/French-position-on-international-law-applied-to-cyberspace.pdf.

50. Roy Schöndorf, *Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations*, 97 INTERNATIONAL LAW STUDIES 395, 401 (2021).

future. However, this does not end the analysis. As discussed previously, encryption of certain types of data may cause a loss of system functionality, even if only temporarily. This result implicates another condition precedent to applying the rule of distinction: the requirement for an attack.

B. Attacks and Distinction

As stated above, civilian objects are protected from attacks under IHL. The wording here is essential as Additional Protocol I defines attacks as "acts of violence against the adversary, whether in offence or in defence."[51] This definition is not nearly as encompassing as might be presumed. Therefore, without the infliction of violence, rules predicated on the commission of an attack would not apply. This logical conclusion provides context to statements, such as those found in the U.S. Department of Defense's *Law of War Manual*, that when "a cyber operation constitutes an attack, then the law of war rules on conducting attacks must be applied to those cyber operations."[52] Furthermore, "such operations must comport with the requirements of distinction and proportionality."[53] These statements suggest that not all malicious cyber operations in armed conflicts must follow the rules related to attacks, such as distinction.

While the *Law of War Manual* does not provide explicit definitions of these terms or concepts, it does give some examples and factors to consider. To begin, "a cyber attack that would destroy enemy computer systems could not be directed against ostensibly civilian infrastructure."[54] It does not define "destroy" but presumably includes the impossibility of using the system again. Conversely, the *Law of War Manual* lists cyber operations that would fail to qualify as attacks, including defacing government webpages, minor disruption of internet services, brief disruption of communications, and propaganda dissemination.[55] While this list is not exhaustive, it suggests that the length and level of disruption are factors to consider. Finally, to use an oft-repeated phrase: are the operations "temporary and reversible?" Of additional note (and without citation), the *Law of War Manual* does state that even for operations that fail to qualify as an attack, cyber operations "should

51. AP I, *supra* note 39, art. 49(1).

52. OFFICE OF THE GENERAL COUNSEL, U.S. DEPARTMENT OF DEFENSE, LAW OF WAR MANUAL § 16.5.1 (rev. ed. Dec. 2016).

53. *Id.*

54. *Id.*

55. *Id.* § 16.5.2.

not be conducted in a way that unnecessarily causes inconvenience to civilians or neutral persons."[56] While this suggests broad protections for civilian data, it should be recalled that the *Law of War Manual* has been criticized for frequently blending law and policy without clear delineations.[57]

Although the United States has yet to provide definitive guidance on when a cyber operation qualifies as an attack, other States are beginning to do so. New Zealand, for example, defines an attack as the "loss of functionality, equivalent to that caused by a kinetic attack."[58] This addition is not further explained but suggests some level of loss of functionality by non-violent means would be included. However, equivalency to a kinetic attack also suggests a more permanent effect. France provides a clear standard, but one that goes further than other States, including in its definition when "the targeted equipment or systems can no longer provide the service for which they were implemented, including temporarily or reversibly, where action by the adversary is required to restore the infrastructure or the system."[59] This definition is quite broad and would include operations such as denial-of-service. On the other hand, Israel takes a stricter approach requiring physical damage to qualify as an attack and excluding "the mere loss or impairment of functionality to infrastructure."[60] These clarifications by States are notable because they are quite divergent and because they are among a small handful of State clarifications on the position.

While States, generally, and military manuals, specifically, have provided few clear definitions for attacks in the cyber context, academics have generated a significant amount of scholarship on the question.[61] The critical issue under debate is whether cyber operations resulting in effects that do not meet traditional notions of violence may qualify. The *Tallinn Manual* drew

---

56. *Id.*

57. *See generally* WILLIAM BOOTHBY & WOLFF HEINTSCHEL VON HEINEGG, THE LAW OF WAR: A DETAILED ASSESSMENT OF THE US DEPARTMENT OF DEFENSE LAW OF WAR MANUAL (2018).

58. New Zealand Ministry of Foreign Affairs and Trade, *The Application of International Law to State Activity in Cyberspace* (Dec. 1, 2020), https://www.mfat.govt.nz/assets/Peace-Rights-and-Security/International-security/International-Cyber-statement.pdf.

59. Paper Shared by France with the Open-Ended Working Group, *supra* note 49, at 12.

60. Schöndorf, *supra* note 50, at 400.

61. *See, e.g.*, WILLIAM H. BOOTHBY, THE LAW OF TARGETING (2012); Michael N. Schmitt, *Rewired Warfare: Rethinking the Law of Cyber Attack*, 96 INTERNATIONAL REVIEW OF THE RED CROSS 893 (2014); Knut Dörmann, *Applicability of the Additional Protocol to Computer Network Attack*, INTERNATIONAL COMMITTEE OF THE RED CROSS (Nov. 9, 2004), http://www.icrc.org/eng/resources/documents/misc/68lg92.htm.

heavily on the language of AP I when it defined a cyber-attack as a "cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects."[62] The *Tallinn Manual* definition, or close approximations thereof, reflects a baseline for the position of most States regarding the application of attacks to cyberspace. However, it leaves open the question of what constitutes "damage or destruction" when discussing information systems generally and data in particular. Because significant variance exists among legal experts on this question, analyzing various categories of effects is useful.

It is uncontroversial that cyber operations, including ransomware operations, that result in violent, physical damage to objects or people qualify as an attack.[63] For example, a cyber-operation against the networked controls of industrial systems resulting in material damage to the equipment would clearly qualify. This is so despite the offensive cyber actor accomplishing the physical damage through non-kinetic means: the remote insertion of malicious code. More problematic is the case of harm to systems that do not produce physical effects, such as loss of functionality to computer systems.[64] There is a certain inherent logic to finding that a malicious operation resulting in a non-functional system constitutes an attack. The result of rendering a functional system non-functional by an opposing actor bears an analogy to kinetic, forceful activities. However, even loss of functionality may operate at differing levels requiring separate analysis. For example, the loss of functionality may require the replacement of physical cyber infrastructure such as hardware components. Similarly, recovering functionality may require reinstalling software components, whether at the operating system or application levels. However, it may only require reentering certain data sets necessary to run the required functions. Each potential remedy to loss of functionality presents different standards of what might trigger an attack. Lacking

62. TALLINN MANUAL 2.0, *supra* note 7, r. 92.

63. *Id.*; DOD LAW OF WAR MANUAL, *supra* note 52, § 16.5.1.

64. The ICRC breaks the different views into the following categories:

> One view is to consider that cyber attacks are only those operations that cause violence to persons or physical damage to objects. A second approach is to make the analysis dependent on the action necessary to restore the functionality of the object, network or system. A third approach is to focus on the effects that the operation has on the functionality of the object.

Int'l Comm. of the Red Cross, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts* 41–42 (2015), https://www.icrc.org/en/download/file/15061/32ic-report-on-ihl-and-challenges-of-armed-conflicts.pdf.

any consensus are cyber operations resulting in effects below the level of loss of functionality.[65] States and scholars have debated the benefits and disadvantages of each of these thresholds. It is not the intent of this article to resolve that debate. Instead, it raises the point that ransomware presents an additional factor that the previous positions would fail to resolve—intentionally reversible and potentially temporary effects.

The use of ransomware by a sophisticated actor is likely to result in encrypted data that the system owner cannot decrypt within a useful period. While the effects of many cyber operations are theoretically reversible, ransomware operations differ in several aspects. First, ransomware rarely causes physical damage as it would be quite contrary to the purpose of ransomware to do so. The intent is to maintain the ability to restore the user to their previous status upon meeting the stated condition. Causing physical damage that cannot be undone by releasing access to data back to the original user would defeat its very purpose. Contrarily, temporary loss of functionality is the desired goal of the offensive operator. Whereas other operations may delete or corrupt data resulting in loss of functionality, a ransomware operation is designed to lock the user out from utilizing a network, application, or data resident on a system until the operator decides to release the encryption. At that point, the target user should regain functionality and access to the data. Reloading software or replacing hardware, the standards typically associated with the loss of functionality test for legal purposes, are not quite the same as ransomware.

Ransomware, however, holds a key difference from other types of temporary and reversible effects. Primarily, there is no time limitation on the restoration of access. Barring the development of quantum computing, the time it would take to break advanced encryption will likely outlast many armed conflicts. While continuous operational denial is theoretically possible with more traditional military operations such as communications jamming or more recent denial-of-service cyber operations, those operations require continuing action by the offensive party. Ransomware requires no such action, making it more probable that the effects will continue for an extended period should the targeted State not comply with the conditions for releasing the data. Referring back to the DoD *Law of War Manual's* examples of cyber operations that would not be held to be an attack, it used words such as

65. TALLINN MANUAL 2.0, *supra* note 7, at 418.

"minor" and "brief" denial operations to describe the non-qualifying effects.[66] Other State views on what constitutes temporary and reversible effects are rather varied. France, for example, takes perhaps the strongest view, finding that any effect causing the system not to operate as intended constitutes an attack.[67] Thus, whether the nature of the effect is temporary or reversible would be irrelevant to the analysis. While there may not yet be enough consensus among State positions to determine what constitutes an attack in these scenarios, the law appears to be moving towards extended denial of functionality as a qualifying effect.

Second, ransomware does not destroy or even damage data, it encrypts it. The offensive operator preserves the data for future use. It is similar to locking someone out of their car. Locking them out renders the vehicle useless to the owner, but no damage has occurred. Taking the analogy further, suppose an army prevents a portion of the civilian population from utilizing private automobiles during the conflict. The act inconveniences the populace, and the law may prohibit the action in certain circumstances (i.e., emergency vehicles). Still, the action is unlikely to be considered an attack for purposes of IHL. However, there are other ways to categorize encryption than as an attack. International law also governs the seizure of property during armed conflicts[68] and the confiscation of property during times of occupation.[69] Given that this article focuses on the uses of ransomware in armed conflicts, only the former will be addressed.

Rule 50 of the Customary International Law study by the International Committee of the Red Cross (ICRC) states that "the destruction or seizure of the property of an adversary is prohibited unless required by imperative military necessity." The Geneva Conventions find a grave breach where there is "extensive destruction and appropriation of property, not justified by military necessity and carried out unlawfully and wantonly."[70] This rule

66. DOD LAW OF WAR MANUAL, *supra* note 52, ¶ 16.5.2.

67. Przmyslaw Roguski, *An Overview of International Humanitarian Law in France's New Cyber Document*, JUST SECURITY (Sept. 27, 2019), https://www.justsecurity.org/66318/an-overview-of-international-humanitarian-law-in-frances-new-cyber-document/.

68. CUSTOMARY INTERNATIONAL HUMANITARIAN LAW, *supra* note 32, r. 50.

69. *Id.* r. 51.

70. Convention (I) for the Amelioration of the Condition of the Wounded and Sick in the Armed Forces in the Field art. 50, Aug. 12, 1949, 6 U.S.T. 3114, 75 U.N.T.S. 31 [hereinafter GC I]; Convention (II) for the Amelioration of the Condition of the Wounded, Sick, and Shipwrecked Members of Armed Forces at Sea art. 51, Aug. 12, 1949, 6 U.S.T. 3217, 75 U.N.T.S. 85 [hereinafter GC II]; Convention (IV) Relative to the Protection of Civilian Persons in Time of War art. 147, Aug. 12, 1949, 6 U.S.T. 3516, 75 U.N.T.S. 287.

raises multiple definitional problems. First, is data considered property for purposes of IHL? Second, is the encryption of data the same thing as a seizure or an appropriation? A similar analysis to the issue of "data as an object" arises as to the former. The law does not generally consider data as personal or real property because it is not tangible.[71] Thus, most prosecutions for "stealing" data are charged domestically as intellectual property crimes or computer trespass crimes, not theft of personal or real property. This analysis appears to extend to the IHL realm. When discussing the appropriation of civilian property in its 2016 commentary to the first Geneva Convention, the ICRC *Commentary* refers to Additional Protocol I discussions of objects.[72] This relationship between objects and property in IHL is logical. Generally, the law protects a user's data only for privacy protection or as intellectual property. Currently, no such protections for privacy or intellectual property exist under IHL.[73] While the encryption of data requires access to the system holding that data, the primary point of using ransomware is to interfere with the use of the data, not to release or otherwise exploit it for the purposes of violating privacy. While it is true that some criminal organizations threaten to release the data if the ransom is not paid, this is a separate legal issue from that covered here.

Regarding the question of whether the encryption of data is the same thing as a seizure or appropriation, there is a strong argument that encryption would qualify as a seizure should the law recognize data as personal property. While the ransomware operator does not technically remove the data from its location, the encryption does establish a certain level of control over the data. *Black's Law Dictionary* defines appropriation as "the exercise of control over property."[74] Additionally, most legal analysis of a seizure focuses on the fact that while data may be copied and acquired by another party, the use of

71. There have been calls from scholars to view data as personal property. *See, e.g.*, Jeffrey Ritter & Anna Mayer, *Regulating Data as Property: A New Construct for Moving Forward*, 16 DUKE LAW AND TECHNOLOGY REVIEW 220 (2020).

72. INT'L COMM. OF THE RED CROSS, COMMENTARY ON THE FIRST GENEVA CONVENTION: CONVENTION (I) FOR THE AMELIORATION OF THE CONDITION OF THE WOUNDED AND SICK IN THE ARMED FORCES IN THE FIELD ¶ 3006 (2016).

73. *See generally* Asaf Lubin, *The Rights to Privacy and Data Protection Under International Humanitarian Law and Human Rights Law*, *in* RESEARCH HANDBOOK ON HUMAN RIGHTS AND HUMANITARIAN LAW: FURTHER REFLECTIONS AND PERSPECTIVES 463–92 (Robert Kolb et al. eds., 2022).

74. *Appropriation*, BLACK'S LAW DICTIONARY (11th ed. 2019).

the data is not denied to the original owner.[75] In the case of ransomware, the operator denies the use of the data to its owner for as long as the encryption remains in place. This places the operation much closer to the traditional understanding of a seizure.

There are powerful arguments on both sides of the debate regarding what constitutes an attack in the cyber domain. The ICRC sums up one side eloquently, stating that "an overly restrictive understanding of the notion of attack would be difficult to reconcile with the object and purpose of the rules on the conduct of hostilities."[76] However, without clear statements of *opinio jurius* to expand the current definition of attacks beyond the limitation of violent effects, such a definitional expansion would be inconsistent with the requirement to interpret treaties within the "ordinary meaning to be given to the terms of the treaty in their context," despite the additional obligation for interpretation "in the light of its object and purpose."[77] Additionally, the definitional expansion would fail to solve the additional complexities presented by ransomware operations. However, distinction is not the only rule potentially applying to civilian data in armed conflicts. Specific categories of civilian data receive protections that do not rely on the qualifications of objects or attacks. The following section addresses these "special protections."

V. SPECIAL PROTECTIONS

While IHL generally seeks to balance the requirements of military operations with the need to protect civilians from grave harm during armed conflicts, there are several categories of persons or objects that States have deemed appropriate to grant additional protections. As a general rule, these categories are freed from the previously discussed requirements of constituting an "attack" or being deemed an "object." Instead, there is a greater emphasis on interference with the function or nature of the category. For this reason,

75. *See* United States v. Gorshkov, No. CR00-550C, 2001 U.S. Dist. LEXIS 26306, 2001 WL 1024026 (W.D. Wash. May 23, 2001). The remote copying of a defendant's computer located outside the United States did not constitute a seizure under the Fourth Amendment because it did not interfere with the defendant's ability to use the computer. *But see* Susan W. Brenner & Barbara A. Frederiksen, *Computer Searches and Seizures: Some Unresolved Issues*, 8 MICHIGAN TELECOMMUNICATIONS & TECHNOLOGY LAW REVIEW 39, 111–12 (2002), arguing that copying digital files interferes with possessory interest and should be treated as a seizure under the Fourth Amendment.

76. *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts*, *supra* note 64, at 41.

77. Vienna Convention on the Law of Treaties, *supra* note 45, art. 31(1).

the law employs terminology such as "respect and protect" instead. These categories include cultural property, civilian journalists, medical units, religious sites, installations containing dangerous forces, civil defense units, and objects indispensable to the civilian populace (including food with an eye towards starving the civilian populace). Additionally, there is a prohibition on the collective punishment of civilians. While not all categories of special protections implicate the potential use of ransomware against civilian data during armed conflicts, many do and are addressed below.

A. Digital Cultural Property

Cultural property protections find original expression in a 1954 Hague Convention. Article 1 of the Convention for the Protection of Cultural Property in the Event of Armed Conflict defines cultural property as "property of great importance to the cultural heritage of every people."[78] High contracting parties of this convention are obligated to "respect" such property.[79] While this may not seem to convey protections for civilian data, the rise of non-fungible tokens (NFT) may obtain such status in the future.[80] As recently as 2021, an NFT sold for over $69 million at auction, raising the question of whether NFTs may become as valuable as other "priceless" works of art.[81]

The *Tallinn Manual* rule related to this provision addresses both cultural property that might be affected by cyberspace operations and cultural property located in cyberspace.[82] It is quite interesting that the issue of intellectual property is briefly mentioned in this section in terms of whether it may ever constitute cultural property. The *Manual* notes that intellectual property is a concept that is accepted in international law generally but does not raise its

78. Convention for the Protection of Cultural Property in the Event of Armed Conflict, May 14, 1954, T.I.A.S. 09-313.1, 249 U.N.T.S. 240; Protocol to the Hague Convention for the Protection of Cultural Property in the Event of Armed Conflict, May 14, 1954, 249 U.N.T.S. 358; Second Protocol to the Hague Convention for the Protection of Cultural Property in the Event of Armed Conflict, Mar. 26, 1999, 2253 U.N.T.S. 172.

79. Convention for the Protection of Cultural Property in the Event of Armed Conflict, *supra* note 78, art. 4.

80. Kevin Roose, *Why Did Someone Pay $560,000 for a Picture of My Column?,* NEW YORK TIMES (updated Aug. 12, 2021), https://www.nytimes.com/2021/03/26/technology/nft-sale.html.

81. Langston Thomas, *The 20 Most Expensive NFT Sales of All Time*, NFT NOW (June 16, 2023), https://nftnow.com/features/most-expensive-nft-sales/.

82. TALLINN MANUAL 2.0, *supra* note 7, r. 142.

application in IHL. In any case, should a digital file constitute protected cultural property, then "any damage, deletion, or destruction of the data, as well as its exploitation for military purposes" would be prohibited.[83] While encryption is not damage, deletion, or destruction, its use in a ransomware operation should be considered "exploitation for military purposes."

B. Medical Data

Medical data is among the most important categories of data that receive protection under IHL. The Geneva Conventions provide special protections to medical units under Article 19 of the First Geneva Convention, stating that those units "of the Medical Service may in no circumstances be attacked, but shall at all times be respected and protected by the Parties to the conflict."[84] Again, the "respect and protect" language suggests a greater degree of protection that goes beyond that which requires an attack. These protections include interfering with the function of specially protected units, including medical units.[85] This position is reflected in the DoD *Law of War Manual*, which provides that medical units and personnel must not be "unnecessarily prevented from discharging their proper functions."[86] This protection includes not only data related to medical treatment, such as that covered under domestic statutes such as the Health Insurance Portability and Accountability Act, but any data that would interfere with the functionality of medical or similar units, medical depots, and associated transport.[87] It should also be noted that this protection has been extended under Additional Protocol I and customary IHL to all medical units during an armed conflict, whether military or civilian.[88] As such, networks and data integral to medical operations or administration must be considered off-limits to all malicious cyber operations, including ransomware.[89]

---

83. *Id.* at 536.

84. GC I, *supra* note 70, art. 19.

85. COMMENTARY ON THE FIRST GENEVA CONVENTION, *supra* note 72, ¶¶ 1799, 1804.

86. DOD LAW OF WAR MANUAL, *supra* note 52, ¶ 7.8.2.

87. GC I, *supra* note 70, arts. 24, 25, 35, 36.

88. CUSTOMARY INTERNATIONAL HUMANITARIAN LAW, *supra* note 32, r. 28; AP I, *supra* note 39, art. 12(2).

89. *See also* TALLINN MANUAL 2.0, *supra* note 7, r. 132.

C. Religious Data

The Geneva Conventions provide special protections to "chaplains attached to the armed forces" under Article 24 of the First Geneva Convention, stating that chaplains shall be respected in all circumstances."[90] Religious data presents a couple of interesting issues related to the use of ransomware. First, the special protections related to religious personnel only extend to those providing ministry to the armed forces, medical units, and civil defense organizations.[91] This narrowing contrasts with medical units, for whom the protected class is much broader. Second, the protection applies specifically to personnel providing ministry to the armed forces of a party to a conflict, as opposed to equipment or units. In other IHL contexts, this would likely limit the protection of data required to perform the functions of the ministry. However, given the "respect and protect" language found in the treaties, this indicates that any interference with the function of these personnel would be prohibited.[92] For example, if ransomware interfered with the provision of online access to religious materials by a chaplain, that would constitute a violation.

Similarly, information systems used by chaplains to coordinate religious care for the armed forces would be protected from any malicious cyber operations that would interfere with those services. The *Tallinn Manual* provides another potential example of a violation: the interference with religious broadcasts through cyber means.[93] However, there are not any special IHL protections that extend to similar classes of civilian religious data.[94]

D. Journalists

The extent to which IHL protects journalists is an area of some dispute. Additional Protocol I, Article 79, provides that journalists in dangerous professional missions shall be considered civilians and protected as such. There is no "respect" language in the treaty for journalists, as seen with medical

90. GC I, *supra* note 70, art. 24.

91. *Id.*; GC 2, *supra* note 70, art. 37; AP I, *supra* note 39, arts. 8(d), 15.

92. AP I, *supra* note 39, art. 1.

93. TALLINN MANUAL 2.0, *supra* note 7, at 514.

94. COMMENTARY ON THE ADDITIONAL PROTOCOLS OF 8 JUNE 1977 TO THE GENEVA CONVENTIONS, *supra* note 44, ¶¶ 637–38.

and religious personnel. However, the ICRC's Customary International Humanitarian Law study does include the "respect and protect" phraseology.[95] In addition, the discussion in the study briefly mentions "journalists exercising their professional activities," but focuses primarily on the physical safety of journalists as opposed to interference with their work as journalists. This apparent contradiction raises the question of whether the protection of journalists extends beyond protection from attack and their physical safety to interference with their journalistic activities.[96]

E. Installations Containing Dangerous Forces

This category presents an interesting issue as the prohibition in Additional Protocol I, Article 56, is against the attack of "installations containing dangerous forces, namely dams, dykes, and nuclear electrical generating stations . . . if such attack may cause the release of dangerous forces and consequent severe losses among the civilian population." Whereas this provision appears to lead the analysis back to questions of attacks in the cyber context, the issue here resolves itself. If a ransomware operation were to somehow result in the release of dangerous forces and severe losses to the civilian population, the ransomware operation would resultantly qualify as an attack. Again, if any cyber operation results in violence, it must be considered an attack under Article 49 of Additional Protocol I. Conversely, a ransomware operation that failed to release dangerous forces resulting in civilian losses would neither qualify as an attack nor violate Article 56 even if it were to qualify as an attack.

F. Civil Defense

Civil defense organizations perform humanitarian tasks "intended to protect the civilian population against the dangers and to help it to recover from the immediate effects of hostilities or disasters and also to provide the conditions necessary for its survival."[97] Among the tasks explicitly included are warning,

95. CUSTOMARY INTERNATIONAL HUMANITARIAN LAW, *supra* note 32, r. 34.

96. A majority of the *Tallinn Manual* IGE took the position that the protections do not extend to journalistic activities, but rather is limited to the journalists themselves. TALLINN MANUAL 2.0, *supra* note 7, at 526.

97. AP I, *supra* note 39, art. 61(a).

evacuation, rescue, and fire-fighting, as well as activities necessary for planning and organizing such tasks.[98] According to Article 62 of Additional Protocol I, civilian civil defense organizations "shall be respected and protected, subject to the provisions of this Protocol, particularly the provisions of this section. They shall be entitled to perform their civil defence tasks except in case of imperative military necessity." Again, an interesting question is raised as to what type of imperative military necessity would be required to prevent such organizations from performing their service. Military necessity can be difficult to define and apply as it is generally considered a part of Article 52(2) of Additional Protocol I's definition of a military objective. However, two key phrases in that definition are helpful if borrowed for the limited purpose of defining military necessity in the context of Article 62.[99] First, there must be "an effective contribution to military action." Second, the action must, "in the circumstances ruling at the time, offer[] a definite military advantage." Here, a generalized desire to end a conflict by affecting civilian morale would not suffice to meet such a requirement and therefore overcome the requirement for "imperative military necessity."

G. Objects Indispensable to the Civilian Populace

The special protections for this category are interesting in the context of ransomware. They include the prohibition in Additional Protocol I, Article 54(2):

> It is prohibited to attack, destroy, remove or render useless objects indispensable to the survival of the civilian population, such as foodstuffs, agricultural areas for the production of foodstuffs, crops, livestock, drinking water installations and supplies and irrigation works, for the specific purpose of denying them for their sustenance value to the civilian population or to the adverse Party, whatever the motive, whether in order to starve out civilians, to cause them to move away, or for any other motive.

Thus, ransomware with the specific purpose of rendering useless a computer system that is required for the production of food, or some other object

98. *Id.*

99. Otherwise, the phraseology applies in the context of attacks and objects, as previously discussed.

indispensable to the survival of the civilian population, would be strictly prohibited. This requirement is generally considered to be customary in nature.[100]

H. Collective Punishment

The prohibition against collective punishment is perhaps the most interesting special protection in the context of using ransomware against civilian targets in armed conflicts. Whereas the previous categories applied to relatively narrow categories of individuals or types of targets, collective punishment is broadly applicable. The applicable rule against collective punishments is found both in international agreements and customary international law. Article 33 of the Fourth Geneva Convention requires that "[n]o protected person may be punished for an offence he or she has not personally committed. Collective penalties and, likewise, all measures of intimidation or of terrorism are prohibited. Pillage is prohibited. Reprisals against protected persons and their property are prohibited."[101] Article 75(2) of Additional Protocol I prohibits "collective punishments" from taking place "at any time and in any place whatsoever." The 1987 *Commentary to Additional Protocol I* adds that the "concept of collective punishment must be understood in the broadest sense: it covers not only legal sentences but sanctions and harassment of any sort, administrative, by police action or otherwise."[102] Finally, this prohibition is generally considered to constitute customary international law.[103]

The implication here is clear. If ransomware operations affecting civilian targets are considered a collective punishment, they would be categorically prohibited in armed conflicts. However, it is unclear if such ransomware operations should be regarded as retaliatory if they have a clear motivation related to the armed conflict other than punishment and penalty for the civilian populace. Retaliation or punishment indicates that it is a response by a party to the conflict to an act committed by some portion of the populace against its interests. A clear historical example is the punishment of civilians for the actions of saboteurs or underground operatives that are presumed to have a

100. *See* CUSTOMARY INTERNATIONAL HUMANITARIAN LAW, *supra* note 32, r. 54.

101. A similarly worded protection also exists in Convention (III) Relative to the Treatment of Prisoners of War art. 87, Aug. 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135.

102. COMMENTARY ON THE ADDITIONAL PROTOCOLS OF 8 JUNE 1977 TO THE GENEVA CONVENTIONS, *supra* note 44, ¶ 3055.

103. CUSTOMARY INTERNATIONAL HUMANITARIAN LAW, *supra* note 32, r. 103.

relationship to the punished population. While ransomware could undoubtedly be used as a retaliatory mechanism, it need not be used that way. Instead, it may be used strategically to push the populace towards reduced support for continuing the conflict. However, if the civilian populace is being penalized for their State's general entry into the conflict or the circumstances leading up to the conflict, then it is unlikely that the civilian populace can be regarded as responsible for those actions.

VI. TARGETING WAR-SUSTAINING OBJECTS

Another relevant issue likely to be raised by the use of ransomware against non-military objectives in armed conflicts is the targeting of "war-sustaining" targets. The analysis here is applicable if ransomware operations against data are to be considered attacks and data is considered an object. To make the best strategic use of ransomware in an armed conflict, States will likely target those objects of the highest economic and societal importance. Economic targets of this type are often analyzed as "war-sustaining" objects, defined by Michael Schmitt as "activities that undergird a war effort, such as the export of items that generate income, allowing the eventual funding of the war effort."[104]

IHL scholars often divide military objects into three categories: war-fighting, war-supporting, and war-sustaining.[105] War-fighting objects are those directly used to engage in military action during armed conflicts, such as military weapons and supplies. As a general matter, there is no question that these objects constitute valid military objectives in an armed conflict. War-supporting objects contribute to producing military supplies and equipment but are not objects used to conduct hostilities. Munitions and weapons factories provide the most evident example. Still, the category could also include facilities such as oil refineries if the products of those facilities are intended for military units or activities. Because of the direct link to military activities, there is general acceptance that they constitute lawful targets. War-

104. Michael N. Schmitt, *Deconstructing Direct Participation in Hostilities: The Constitutive Elements*, 42 NEW YORK UNIVERSITY JOURNAL OF INTERNATIONAL LAW AND POLITICS 697, 718 (2010). *See also* Israel D. King, *The Legality of Attacking War-Sustaining Economic Objects*, 54 STANFORD JOURNAL OF INTERNATIONAL LAW 49, 51 (2018).

105. Michael N. Schmitt, *Peacetime Cyber Responses and Wartime Cyber Operations Under International Law: An Analytical Vade Mecum*, 8 HARVARD NATIONAL SECURITY JOURNAL 239, 269 (2017).

sustaining objects, however, lack that direct link. Instead, these objects support the war effort by providing significant revenue to fund military operations, including payment to combatants and purchasing war-supporting materials. An often-debated example was the oil produced by the Islamic State that was not destined for direct use by their armed groups. Rather, the Islamic State sold significant oil to fund various aspects of their group, including military operations.[106] Strikes against these targets generated much debate in the academic community.[107]

States are divided on the question of war-sustaining objects. The United States explicitly includes the war-sustaining objects in its definition of a military objective.[108] While most States do not expressly support or deny the U.S. position, it has received wide criticism focusing on Additional Protocol I's requirement in Article 52(2) for a military objective to "make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage." This article does not seek to resolve this difficult question of law but only to point out that should a ransomware operation be considered an attack, or if data were to be considered an object, the war-sustaining issue would almost certainly come into play.

VII. NORMATIVE LIMITATIONS

Thus far, this article has outlined the argument that there are no explicit legal prohibitions on the strategic use of ransomware against civilian targets in armed conflicts. Of course, international law is not the only check on State behavior during armed conflicts. Just because an operation meets legal requirements does not necessarily mean a State should conduct the operation. Norms of international behavior, driven by policy and ethical considerations, also come into play. In recognizing potential legal gaps related to civilian data

106. Ana Swanson, *How the Islamic State Makes Its Money*, WASHINGTON POST (Nov. 18, 2015), https://www.washingtonpost.com/news/wonk/wp/2015/11/18/how-isis-makes-its-money/.

107. *See, e.g.*, Kenneth Watkin, *Sustaining the War Effort: Targeting Islamic State Oil Facilities*, JUST SECURITY (Oct. 3, 2014), https://www.justsecurity.org/15890/sustaining-war-effort-targeting-islamic-state-oil-facilities/.

108. DOD LAW OF WAR MANUAL, *supra* note 52, ¶ 5.7.6.2. *See also* 10 U.S.C. § 950p(a)(1) ("The term 'military objective' means . . . those objects during hostilities which, by their nature, location, purpose, or use, effectively contribute to the war-fighting or war-sustaining capability of an opposing force").

in armed conflicts, Michael Schmitt recently offered several potential normative limitations.[109] His first recommendation is "to accord special protection to certain 'essential civilian functions or services' by committing to refrain from conducting cyber operations against civilian infrastructure or data that interfere" with those functions or services.[110] Additional categories included in this protection beyond those already identified as receiving special protections include: "the delivery of social services to the disabled, young, poor and elderly" as well as "primary and secondary education."[111] This is a sensible approach from both a policy and strategy standpoint. Such targets would likely fail to serve the strategic interests of a State in any case.

Schmitt's second proposal asks States to "commit, as a matter of policy, to refraining from conducting cyber operations to which the IHL rules governing attacks do not apply when the expected concrete negative effects on individual civilians or the civilian population are excessive relative to the concrete benefit related to the conflict that is anticipated to be gained through the operation."[112] In the context of strategic ransomware operations, this formulation would be challenging to apply. If successful, the "concrete benefit" would likely outweigh any "concrete negative effects," particularly given the inherently reversible nature of ransomware. The real question is whether an outcome as speculative as the demanded terms of the ransom could ever be considered concrete. Nevertheless, such a policy agreement would likely take certain targets off the table that would be deemed particularly cruel towards the civilian population.

VIII. CONCLUSION

Although States have yet to use ransomware in armed conflicts, cyber-enabled information warfare in armed conflicts has increased. There is no reason to think that, at some point, a State may attempt to utilize a technique for military purposes that has proven so successful in the criminal context. The advantage of ransomware as a technique of warfare relative to other types of cyber operations lies in its coerciveness. Unlike most cyber operations, which are exploitive in nature, ransomware has the potential to force the opponent into a particular and pre-determined set of actions. Additionally, the recipient

109. *See* Michael N. Schmitt, *Wired Warfare 3.0: Protecting the Civilian Population During Cyber Operations*, 101 INTERNATIONAL REVIEW OF THE RED CROSS 333 (2019).

110. *Id.* at 345.

111. *Id.* at 347.

112. *Id.* at 349.

knows that accepting the terms of the ransom may result in an immediate resumption of the status quo. This is unlike kinetic activities such as bombing campaigns, which are not so easily undone.

Not only is ransomware a potentially useful strategic technique, but States are likely to exploit the legal ambiguities of ransomware under IHL. Concepts such as defining attacks and objects, the extent of certain special protections, and the status of war-sustaining objects already exist under a cloud of legal uncertainty. The very nature of ransomware effects, which are potentially debilitating but also temporary and reversible, exacerbate this legal uncertainty. For example, should a consensus develop that non-violent cyber operations that nevertheless cause permanent loss of functionality to an information system qualify as attacks, that would still fail to resolve the ransomware issue. Are ransomware operations more like temporary denial of service operations, which find little support to be labeled as attacks? Or is the potential for permanent (or at least extended) loss of functionality enough to change the equation?

At this stage, State practice and *opinio juris* relating to cyber operations are insufficient to find a definitive prohibition on ransomware operations against most civilian targets during armed conflicts. While special protections exist for several essential categories, such as medical units and objects indispensable to the civilian populace, it is currently left to normative, not legal, limitations to protect most civilian data from ransomware operations during armed conflicts. Responsible States should make a concerted effort to push normative constraints protecting additional categories of civilian data, such as those recommended by Michael Schmitt. Although this answer is likely unsatisfying to many, it is a necessary step toward developing more definite legal protections during armed conflicts.