CYBER PILLAGE

Christopher Greulich*
Eric Talbot Jensen**

* Juris Doctor, Brigham Young University Law School.
** Robert W. Barker Professor of Law, Brigham Young University Law School. The authors would like to express gratitude to Summer Crockett for her excellent research assistance and substantive review.

I. INTRODUCTION

In early 1258, the Mongols gathered outside the walls of Baghdad, then probably the largest and most advanced city in the world. On February 10, the Abbasid Caliph, al-Mustasim, made a late attempt to spare the city, but Hulagu Khan rejected this offer. After letting the city sit silent for three days, Hulagu then released his armies into the city, sparing only the Nestorian Christians. Hundreds of thousands of people were killed and many others sold into slavery. The pillage of the city and its citizens by the Mongol army was widespread and complete.[1] According to many historians, the sack of Baghdad signaled the end of the Muslim Golden Era.[2]

This is just one of the notorious historical examples of pillage, a common practice in armed conflict prior to the 19th Century.[3] Not until the 18th Century was there a general recognition that pillage was undesirable among professional armies,[4] as signaled by the Lieber Code that was issued by President Lincoln to the Union forces during the American Civil War, levying the potential punishment of death as a consequence to any who participated in this practice.[5]

Subsequent law of armed conflict ("LOAC") codifications embraced the new proscription and followed the illegalization of pillage. The Oxford Manual,[6] as well as the 1899[7] and 1907 Hague Conventions[8] prohibited

---

1. *E.g.*, GEORGE F. NAFZIGER & MARK W. WALTON, ISLAM AT WAR: A HISTORY 75 (2003).

2. *E.g.*, SEBASTIAN R. PRANGE, MONSOON ISLAM: TRADE AND FAITH ON THE MEDIEVAL MALABAR COAST 17 (2018).

3. *See* TUBA INAL, DEVELOPMENT OF GLOBAL PROHIBITION REGIMES: PILLAGE AND RAPE IN WAR 4 (2008) ("Visigoths pillaged Rome in 409 and Vandals in 455, the Crusaders pillaged Belgrade, lots of villages and towns in the Asia Minor in 1096, Jerusalem in 1099 and Constantinople and the Greek islands in 1204, and the Napoleonic Armies looted Italian towns in 1805-1806 and in return the Russian Army looted the French countryside.").

4. U.S. DEP'T OF DEF., LAW OF WAR MANUAL ¶ 5.17.4.2 (2016) [hereinafter DOD LAW OF WAR MANUAL].

5. GEN. ORD. NO. 100: THE LIEBER CODE INSTRUCTION FOR THE GOVERNMENT OF ARMIES OF THE UNITED STATES IN THE FIELD art. 44 (Apr. 24, 1863) (defining the acceptable rules of conduct during hostilities for Union soldiers throughout the U.S. Civil War, the orders were issued by President Lincoln and are commonly known as the "Lieber Code," named after its main author, Francis Lieber) (originally issued as General Orders No. 100, Adjutant General's Office, 1863, Washington 1898: Government Printing Office) [hereinafter LIEBER CODE].

6. The Oxford Manual prohibited pillage, as unanimously adopted by the Inst. of Int'l Law, a scientific association composed of a fixed number of members and associates of different nations and whose mission is to aid the gradual and progressive codification of international law. Gustave Moynier, *Oxford Manual of the Laws of War on Land*, 5 ANNUAIRE DE L'INSTITUT DE DROIT INT'L 157, 164 (1881/82) [hereinafter Oxford Manual].

pillage. More modern instantiations not only prohibit the practice, but also attach both individual criminal liability[9] for participating in pillage and command responsibility for leaders that fail to prevent such conduct.[10] The prohibition is so settled that the International Committee of the Red Cross ("ICRC") has determined that the practice of pillage is prohibited in both international armed conflicts and non-international armed conflicts as a matter of customary international law.[11]

It seems clear at this point that pillage, or the taking of public or private property for private or personal use, is prohibited in armed conflict. This clarity notwithstanding, to address what appropriately has been dubbed "the greatest transfer of wealth in human history,"[12] many are calling for a mass expansion of the theory of pillage. In light of these calls and the rapid emergence of new technologies, it is not as clear how this prohibition will apply to new weapon systems such as those used in cyberspace. This article reviews the elements of pillage in light of cyber operations during armed conflict and argues that cyber pillage remains susceptible to prohibition, and additionally distinguishes between cyber activities that fall under the ban and those that do not.

In light of the public's increased use of the term "pillage" to describe various forms of cyber theft outside the context of an armed conflict, Part II of this paper elucidates the definitional terms applicable to pillage and applies them to cyber activities currently conducted outside the context of an armed conflict against the United States ("U.S.") and its citizens. Part III builds on Part II by describing cyber activities that, if conducted within the context of an armed conflict, would amount to pillage and therefore be prohibited by the LOAC. The article will conclude in Part IV.

---

7. Laws of Customs of War on Land art. 28, 47, July 29, 1899, 32 Stat. 1803, T.S. No. 403 [hereinafter Convention (II)].

8. Laws and Customs of War on Land art. 28, 47, Oct. 18, 1907, 36 Stat. 2277, T.S. No. 539 [hereinafter Convention (IV)].

9. Prosecutor v. Ntaganda, ICC-01/04-02/06, Sentencing Judgment of Judge Fremr, Ozaki, Chung, ¶¶ 133, 143, 151 (Nov. 7, 2019).

10. *See* Prosecutor v. Delalić, IT-96-21-T, Judgment, ¶ 776 (Int'l Crim. Trib. for the Former Yugoslavia Nov. 16, 1998); TIMOTHY BROOK, THE NANKING ATROCITY, 1937-1938, 149 (Bob Tadashi Wakabayashi ed., 2017).

11. 1 JEAN-MARIE HENCKAERTS & LOUISE DOSWALD-BECK, CUSTOMARY INTERNATIONAL HUMANITARIAN LAW, 182 (2005) [hereinafter ICRC Rule 52].

12. *See* The Future of Warfare: Hearing Before the S. Comm. on Armed Serv., 114th Cong. 54-55 (2015) (statement of General Keith B. Alexander, USA, Ret., Former Commander, U.S. Cyber Command and Former Dir. Nat'l Sec. Agency) [hereinafter Statement of General Keith B. Alexander].

II. PILLAGE

As will be discussed further in the Part II(B), pillage is a legal term of art with a long history of being applied only under narrow conditions. For purposes of this paper, the authors will use the LOAC centered definition of "the non-consensual taking of public or private property by members of armed forces during armed conflict for private or personal use," noting that "armed forces" can include both state and non-state actors, or other agents of a Party to the conflict. Further, the authors will not make a distinction between pillage and "looting" or "plunder" as the majority of military manuals treat them as synonyms.[13]

However, contemporary use of the term "pillage" has expanded from its historical meaning. In today's cyber age, common use of the term pillage has transformed form a narrow application of a tactic in armed conflict to a broad description of the theft of digital information involving not only governments, but private actors such as individuals and corporations.[14] This Part examines the dichotomous usage of the two perspectives, concluding that the international law prohibition of pillage remains tied to the more traditional, narrow definition, requiring the existence of an armed conflict.

A. *Transforming Definition of Pillage*

The digital revolution has clearly initiated a transformative wave of growth and development across the entire human experience. Access to knowledge and the ability to collaborate have dramatically increased innovation and development in ways previously impossible. It is undisputed that the internet and its benefits have radically changed the world for the better and allowed progress in ways previously unimagined. However, it has also led to vulnerabilities and risks that can impact global economies and international security in ways its developers would never have predicted. One of the most prominent examples of these new vulnerabilities

13. *E.g.*, DOD LAW OF WAR MANUAL, *supra* note 4; *see also, e.g.*, DIRECTORATE OF LEGAL SERVICES (DLS), MANUAL OF ARMED FORCES LAW, DM 69, VOL. 4 LAW OF ARMED CONFLICT, ¶ 8.10.31 (2019) (N.Z.), http://www.nzdf.mil.nz/downloads/pdf/public-docs/dm_69_2ed_vol_4.pdf [hereinafter New Zealand LOAC Manual]; *see also, e.g.*, MINISTRY OF DEFENCE, MANUAL ON THE LAW OF ARMED CONFLICT, JSP 383, ¶ 15.23 (2013) (Eng.) [hereinafter UK LOAC Manual]; *see also* Prosecutor v. Delalić, IT-96-21-T, Judgment, ¶ 591 (Int'l Crim. Trib. for the Former Yugoslavia Nov. 16, 1998).

14. The authors recognize the two views are not mutually exclusive; some in the latter group are neither private individuals nor corporations. Indeed, some who share the view are government officials. Their views and statements, however, are not attributable to the official U.S. government position on the topic. Therefore, collectively the entire group holding this view will be referred to hereinafter as "the public."

is the cybertheft of intellectual property ("IP"),[15] currency,[16] and other electronic assets.[17]

IP rights deal with "creations of the mind"[18] and are so fundamental that the founding fathers felt compelled to include them in the U.S. Constitution by including, the Congress shall have power "[t]o promote the progress of science and useful arts, by securing for limited times to authors and inventors the exclusive right to their respective writings and discoveries."[19] Yet, cybertheft is the fastest growing category of crime in the U.S.,[20] occurring on a scale unequaled in the history of the world.

The severity of this new vulnerability is evidenced in the economic impact caused by the digital transfer of intellectual property from the U.S. to China. In testimony before the U.S. Senate, General Keith B. Alexander, then Director of the National Security Agency ("NSA") and United States Cyber Command ("USCYBERCOM"), described the theft as "the greatest transfer of wealth in human history."[21] By some estimates, the *annual* economic cost in counterfeit goods, pirated software, and theft of trade secrets in the U.S. alone exceeds $600 billion,[22] and the immediately identifiable and tangible minimum overall cost of IP theft in the U.S. is estimated to be as high as 5% of the U.S. Gross Domestic Product ("GDP") of $18 trillion.[23] These figures, however, include neither the nearly-impossible-to-ascertain costs associated with patent infringement,[24] nor those related to the impact of the job loss resulting from theft of IP, the ratio of which is estimated to be as high as 2.1 million full time jobs lost for

15. Emily Mossburg et al., *The Hidden Costs of an IP Breach*, 19 DELOITTE REV. 106, 108 (2016).

16. *Id.*

17. *Id.*

18. World Intellectual Property Organization, *What is Intellectual Property?*, WIPO PUBLICATION (2018), https://www.wipo.int/edocs/pubdocs/en/intproperty/450/wipo_pub_450.pdf.

19. U.S. CONST. art. I, § 8, cl. 8.

20. Nicolas P. Terry, *Will the Internet of Things Transform Healthcare*, 19 VAND. J. ENT. & TECH. L. 327, 338 (2016).

21. Statement of General Keith B. Alexander, *supra* note 12.

22. Militærmanual Om Folkeret for Danske Væbnede Styrker I Internationale Militære Operationer (Den.), *translated in*, MILITARY MANUAL ON INTERNATIONAL LAW RELEVANT TO DANISH ARMED FORCES IN INTERNATIONAL OPERATIONS ¶ 2.7 (Sept. 2016) (Den.) [hereinafter DANISH MILITARY OPERATIONS].

23. *Update to the IP Commission Report: The Theft of American Intellectual Property: Reassessments of the Challenge and United States Policy*, THE NAT'L BUREAU OF ASIAN RESEARCH 2 **(**Feb**.** 2017), http://ipcommission.org/report/IP_Commission_Report_Update_2017.pdf [hereinafter *IP Comm'n.*].

24. *Id.*

every $48 billion in IP theft.[25] Also excluded from the estimates are a number of intangible and much more difficult to identify costs to U.S. companies and consumers, such as those related to substantially higher expenditures on developing and implementing cybersecurity defenses,[26] which experts predict five-year cumulative spending forecasts will exceed $1 trillion in 2020.[27] Still, despite increased spending on security measures, experts predict the annual cost of cybercrime, including theft of IP, destruction of data, theft of funds, and the associated costs of remediating those harms, will surge to more than $6 trillion by 2021.[28]

The nature and staggering scale of cyber theft understandably causes concern over the unpredictable future impacts these thefts might have. Perhaps it is these impacts which have led some commentators to liken the perpetrators to pirates and to describe the thefts as pillage. U.S. Army scholars, Colonel David Wallace and Lieutenant Colonel Mark Visger, have argued:

> China has pillaged intellectual property from American companies through cyber espionage for decades resulting in the greatest transfer of wealth in human history. It is difficult to overstate the negative impact that such theft has had on American economic growth and prosperity and the ways in which it has undermined America's military and national security.[29]

This view is illustrative of how use of the word "pillage" has evolved from the historically narrower definition discussed in the next section, and how some are using the evolved definition to justify armed response against perpetrators. In order to better understand the way in which pillage has become so freely associated with theft of IP and why its application in that context is insufficient to implicate the LOAC, it is valuable to evaluate two

---

25. The U.S. International Trade Commission estimates that 2011 put the employment loss associated with $300 million in IP theft at the equivalent of 2.1 million full time employees. *See* China: Effects of Intellectual Property Infringement and Indigenous Innovation Policies on the U.S. Economy, Inv. No. 332-519, USITC Pub. 4226 (May, 2011) (final). It is important to note that this estimate is likely on the low end of actual losses, as the USITC Report failed to include "less-IP intensive industries," and it did not have the participation of some of the most vulnerable U.S. companies. Additionally, the report probably vastly underestimated the impact of the theft of trade secrets, where many of the victims are ignorant of the theft or unwilling to report the information, and neither does it include the 5:1 ratio of support jobs created for every IP-intensive role created. *See IP Comm'n.*, *supra* note 23.

26. *IP Comm'n.*, *supra* note 23.

27. *See id.* at 2.

28. Steve Morgan, *2018 Cybersecurity Market Report*, CYBERSECURITY VENTURES (May 31, 2017), https://cybersecurityventures.com/cybersecurity-market-report/.

29. David Wallace & Mark Visger, *Responding to the Call for a Digital Geneva Convention: An Open Letter to Brad Smith and the Technology Community*, 6 J.L. & CYBER WARFARE 3, 47 (2018).

commonly held misconceptions about the concept of pillage. First, there is misconception of the legal meaning of the word "pillage." Second, there is misconception about when and how the intellectual property is stolen, both of which bear on the allowable responses.

1. The Rise of Domestic Pillage

Incorporating domestic theft of intellectual property by cyber means into the meaning of pillage is a view likely fueled by two common associations with another historically meaningful term – piracy. Piracy has long been associated with pillage. After all, in common parlance, pirates are known to "rape, plunder, and *pillage*."[30] Notwithstanding its historical meaning under international law,[31] which is closely linked to theft on the high seas, piracy has taken on a second definition in the last four decades, which associates piracy with infringing on copyrights.[32] It would be difficult to find someone in modern society who has not seen the now-infamous and ever present "FBI Anti-Piracy Warning" at the beginning of nearly every feature film.

Compounding the problem could be a recent change to Black's Law Dictionary's definition of pillage. Though Black's Law Dictionary is not a conclusive source of definitions for international law terms, the ICRC uses Black's Law Dictionary's Fifth Edition to define pillage for purposes of international humanitarian law. Under this definition, pillage is "*the forcible taking of private property by an invading or conquering army from*

30. *Man Knowledge: A Pirate Primer*, ART OF MANLINESS (Mar. 21, 2011), https://www.artofmanliness.com/articles/man-knowledge-a-pirate-primer/.

31. Article 101 of the 1982 UN Convention on the Law of the Sea defines piracy as consisting of any of the following acts:

> (a) any illegal acts of violence or detention, or any act of depredation, committed for private ends by the crew or the passengers of a private ship or a private aircraft, and directed:
>
> (i) on the high seas, against another ship or aircraft, or against persons or property on board such ship or aircraft;
>
> (ii) against a ship, aircraft, persons or property in a place outside the jurisdiction of any State;
>
> (b) any act of voluntary participation in the operation of a ship or of an aircraft with knowledge of facts making it a pirate ship or aircraft;
>
> (c) any act of inciting or of intentionally facilitating an act described in subparagraph (a) or (b).

See Convention on the Law of the Sea, Art. 101, Dec. 10, 1982, 1833 U.N.T.S. 397.

32. *See generally* FBI Anti-Piracy Warning Seal, FBI (ND), https://www.fbi.gov/investigate/white-collar-crime/piracy-ip-theft/fbi-anti-piracy-warning-sea (last visited Apr. 6, 2020).

the enemy's subjects."[33] In contrast, the eleventh, and most recent edition of Black's Law Dictionary, defines pillage as "*[t]he forcible seizure of another's property, esp. in war; esp., the wartime plundering of a city or territory*."[34]

It stands to reason some may see the change as a precursor to a change in customary international law. However, as will be discussed further in Part II(B), the new definition is wholly problematic and is supportable neither under current international law nor historic use of the term for the following reasons. First, "another's property" is too broad to be accurate. Military forces are permitted to take certain property under the LOAC,[35] so despite the property belonging to someone else, the taking of that property may not be pillage. Second, there is no requirement the property taken be converted for personal use, which is a determinative element under international law. Third, international law recognizes there are situations in which force is not a prerequisite to making a finding that pillage has occurred. Finally, and perhaps most important, the definition has no armed conflict requirement at all. "Especially in war" does not mean the same thing as "only in war," and international law requires the existence of an armed conflict to satisfy the elements of pillage. In other words, to accept the current Black's Law definition is to accept that any forcible theft of any property for any purpose by any person at any time is pillage. That is simply not supported in the law. No court has charged, let alone convicted, anyone of pillage outside the context of an armed conflict. What Black's current definition describes is basically robbery,[36] not pillage, and modern cybertheft seldom would rise to a level sufficient to trigger pillage.

Despite the long history of pillage under international law, conflation of the two definitions of pillage is not difficult to understand. Just as with piracy, the word "pillage" has taken on a second definition of its own – one used to describe the mass theft of digital information – and those who incorporate the theft of IP into the definition are not wholly wrong for it. Indeed, just as pillage has a long, binding history under international law, there is an alternate definition with a nearly equally long history that applies domestically. Not surprisingly, the elements of the war crime of pillage are

33. *See* ICRC Rule 52, *supra* note 11 (citing Black's Law Dictionary, at 1033 (5th ed. 1979)) (emphasis added).

34. *See Pillage*, Black's Law Dictionary (Bryan A. Garner, ed., 11th ed. 2019) (emphasis added).

35. *See* Convention (II), *supra* note 7, at art. 52; *see* Convention (IV), *supra* note 8, at arts. 28, 47.

36. *See Robbery*, Black's Law Dictionary (11th ed. 2019) (defining robbery as "[t]he illegal taking of property from the person of another, or in the person's presence, by violence or intimidation…").

not the same as those required to implicate the meaning of domestic pillage, as applied to the theft of IP.

When first used to define theft of intellectual property, pillage involved no armed conflict whatsoever. In this context, "pillage" carried its own unique meaning, one of a wholly domestic and civilly enforceable nature. Even after U.S. laws were modified in 1897 to categorize IP theft as a criminal matter,[37] pillage still was a domestic affair entirely, remedies for which required internal prosecution of offenders. Though IP theft has evolved from requiring a physical presence with the stolen property to an action that can be, and often is, carried out by an actor located outside the U.S., the crime remains a domestic criminal issue.

In *Morrison v. National Australia Bank*, the Supreme Court held, "[u]nless there is the affirmative intention of the Congress clearly expressed to give a statute extraterritorial effect a court must presume it is primarily concerned with domestic conditions… When a statute gives no clear indication of an extraterritorial application, it has none."[38] In other words, unless the specific law the actor violated clearly states its extraterritorial application, U.S. courts do not have the long-arm ability to reach out and grab the actor. Moreover, even if Congress constructed the statute to allow extraterritorial application, the host country of the actor would have to allow for extradition to the U.S. for prosecution, which is hardly the case with the countries that most prolifically conduct these types of attacks; neither China, Russia, North Korea, nor Iran are going to extradite to the U.S., especially when the actors are members of those States' own military or intelligence agencies. Understandably, this is frustrating for victims of IP theft, but international law does not allow escalated responses simply because domestic policy is insufficient to address those frustrations.

2. Other Considerations for Non-Application of Pillage

One of the chief concerns with continued fusing of the definitions is that of unintentional escalation to armed conflict in situations that do not otherwise warrant such response. International law provides two

37. *See* Copyright Act of Jan. 6, 1897, ch. 4, § 4966, 29. Stat. 481, 482 (1897) (criminalizing for the first time, as a misdemeanor, the "unlawful performances and representations of copyrighted dramatic and musical compositions" so long as the violation was "willful and for profit); *see also The Criminalization of Copyright Infringement in the Digital Age*, 112 HAR. L. R. 7, 1705, 1707 (1999) (explaining that the Copyright Act of 1909 greatly expanded the criminal penalties for copyright infringement, in an attempt to stem the increasing number of profit-seeking copyright pirates); *see also* Piracy and Counterfeiting Amendments Act of 1982, Pub. L. 97-180, 96 Stat. 91 (1982) (criminalizing as a felony the copyright infringement of audio and video recordings, punishable by both a $250,000 fine and five year imprisonment).

38. Morrison v. Nat'l Austl. Bank, 561 U.S. 247, 255 (2010) (citation omitted).

circumstances under which a state can resort to force. First, a state may use force when an armed attack has occurred or is imminent, pursuant to Article 51 of the United Nations ("UN") Charter.[39] However, the view that theft of intellectual property conducted by cyber means rises to the level of an armed attack, even at the levels previously described, has not been adopted by the international community.[40]

The second circumstance in which a state can resort to force is upon advisement to and direction of the United Nations Security Council ("UNSC"). Articles 39 and 42 of the U.N. Charter work in concert to authorize the UNSC to direct forceful actions if the UNSC believes (1) the offending act constitutes a threat to the peace, a breach of the peace, or an "act of aggression," and (2) no peaceable solution exists to resolve the conflict.[41] A subjective view of the current threats may suggest the severity of the actions constitutes a threat to, or breach of, the peace, and some may even argue the thefts are acts of aggression. This debate is, however, immaterial; any action authorized under these authorities requires concurrence of the five permanent members of the UNSC, including France, the United Kingdom, the Russian Federation, China, and the U.S.[42] Considering two of the largest offenders are Russia and China, there is little chance of the U.S. obtaining authorization under this mechanism.

Article 25 of the U.N. Charter requires states to comply with the decisions of the UNSC.[43] If the U.S. went against the UNSC decision and took unauthorized forceful action, the U.S. would be accountable for an unjustified armed attack against another nation. Not only would this cause severe deterioration of international alliances and generate costs far in excess of those recognized by IP losses, but also given the likely targets of such an attack, the action carries the distinct possibility of sparking World War III.

Make no mistake, anger over the theft of intellectual property is understandable, and neither the term applied to the theft, nor the means by which it was carried out, can assuage the anger felt by those who experienced the loss; this may be particularly true for someone who just lost the ability to capitalize on the invention of a lifetime. However, each misapplication of the term pillage elevates the risk of overreaction and,

39. U.N. Charter art. 51.

40. *See* TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS, 550-1 (Columbia University Press eds., 2nd ed. 2017) [hereinafter TALLINN MANUAL 2.0].

41. U.N. Charter arts. 39, 42.

42. U.N. Charter art. 25.

43. U.N. Charter art. 24, ¶ 1.

ultimately, of causing massive damage to the U.S. economy that could take years from which to recover. The facts surrounding the theft of IP must be carefully considered before deciding on a responsive course of action, and failure to consider those risks can have grave consequences.

B. *LOAC Application of Pillage*

In contrast to the evolving broad usage of the term, governments continue to view pillage as a narrow prohibition, applicable only to the taking of private property by armed forces for non-military purposes within the context of an armed conflict. For example, Denmark's Law of War Manual describes pillage as "when the members of the armed forces of a party to a conflict unjustifiably appropriate private property for the purpose of making a private gain."[44] The U.S. Law of War Manual defines pillage as "the taking of private or public movable property (including enemy military equipment) for private or personal use. It does not include an appropriation of property justified by military necessity."[45] Other states have similar definitions.[46]

1. Historical Development of the Prohibition on Pillage[47]

Historically, pillage "served as a form of compensation for private armies."[48] Over time, and generally as a matter of exercising discipline on professional armies,[49] pillage and looting were proscribed. The first major prohibition is detailed in the 1863 Lieber Code, promulgated by Francis Lieber, at the request of President Abraham Lincoln. Article 44 states:

> All wanton violence committed against persons in the invaded country, all destruction of property not commanded by the authorized officer, all

44. *See* DANISH MILITARY MANUAL, *supra* note 22, at ¶ 2.7 §407.

45. DOD LAW OF WAR MANUAL, *supra* note 4.

46. *See, e.g.*, AUSTRALIAN DEF. FORCE WARFARE CTR., AUSTRALIAN DEFENSE FORCE PUBLICATION 37 – LAW OF ARMED CONFLICT, ADDP 06.4, ¶ 7.46 (2006) (Austl.); *see also, e.g.*, CHIEF OF DEF. STAFF, LAW OF ARMED CONFLICT AT THE OPERATIONAL AND TACTICAL LEVELS, B-GJ-005-104/FP-021, ¶ 624 (2001) (Can.) (defining pillage as "the violent acquisition of property for private purposes," similarly to Australia); *see also, e.g.*, Manual i krigens folkerett (Nor.), *translated in* MANUAL OF THE LAW OF ARMED CONFLICT ¶ 9.40 (2016) (defining pillage as "taking possession of or stealing property for private purposes… [t]he prohibition applies to all enemy civilian property and effects, whether public or private"); *see also, e.g.*, UK LOAC Manual, *supra* note 13, at ¶ 5.35 2004 (defining pillage as "the obtaining of property against the owner's will and with the intent of unjustified gain").

47. *See* INAL, *supra* note 3, at 37-73 (offering a much more detailed discussion of the history of pillage, including the movement to its modern prohibition).

48. DOD LAW OF WAR MANUAL, *supra* note 4, at ¶ 5.17.4.2.

49. UK LOAC Manual, *supra* note 13, at ¶ 11.76.2; *see* INAL, *supra* note 3, at 24, 63-64.

> robbery, all pillage or sacking, even after taking a place by main force, all rape, wounding, maiming, or killing of such inhabitants, are prohibited under the penalty of death, or such other severe punishment as may seem adequate for the gravity of the offense.
>
> A soldier, officer or private, in the act of committing such violence, and disobeying a superior ordering him to abstain from it, may be lawfully killed on the spot by such superior.[50]

The prohibition on pillage was repeated in the 1874 Brussels Declaration[51] and the 1880 Oxford Manual on the Laws of War on Land.[52] Both the 1899 Hague Convention (II) with Respect to the Laws and Customs of War on Land[53] and its 1907 successor[54] embraced the prohibition on pillage. Both contained the same prohibitions – one, a clear statement that "[p]illage is formally forbidden,"[55] and the other, that "pillage of a town or place, even when taken by assault, is prohibited."[56]

After the massive destruction caused by World War II, the 1949 Geneva Conventions reiterated the prohibition on pillage. Article 16 of the Geneva Convention Relative to the Protection of Civilian Persons in Time of War requires the Parties to take steps to "search for the killed and wounded, to assist the shipwrecked and other persons exposed to grave danger, and to protect them against pillage and ill-treatment."[57] Echoing its Hague predecessors, article 33 of the same convention simply states "[p]illage is prohibited."[58]

While these documents only limit actions in international armed conflicts, Additional Protocol II to the 1949 Geneva Conventions[59] prohibits pillage in the context of non-international armed conflicts. Article 4, paragraph 2 states:

---

50. *See* LIEBER CODE, *supra* note 5, at arts. 22, 37, 38, 47, 72.

51. Project of an International Declaration Concerning the Laws and Customs of War [Declaration of Brussels] (Brussels Conference on the Laws and Customs of War, No. 18) arts. 18, 39, Aug. 27, 1874, 4 Martens Nouveau Recueil (ser. 2) 219.

52. Oxford Manual, *supra* note 6, at art. 32.

53. *See* Convention (II), *supra* note 7.

54. *See* Convention (IV), *supra* note 8.

55. Convention (II), *supra* note 7, at art. 47.

56. Convention (IV), *supra* note 8, at art. 28.

57. Geneva Convention Relative to the Protection of Civilian Persons in Time of War art. 16, Aug. 12, 1949, 6 U.S.T. 3516, 75 U.N.T.S. 287.

58. *Id.* at art. 33.

59. Protocol II Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts art. 4, June 8, 1977, 1977 U.S.T. LEXIS 465, 1125 U.N.T.S. 609.

> Without prejudice to the generality of the foregoing, the following acts against the persons referred to in paragraph 1 are and shall remain prohibited at any time and in any place whatsoever:
>
> g) pillage;[60]

In fact, the ICRC has concluded in its Customary International Humanitarian Law Study that the prohibition on pillage has developed into a current "norm of customary international law applicable in both international and non-international armed conflicts."[61]

This conclusion is confirmed by the International Tribunal for the Former Yugoslavia. In the *Celebici Camp* case, several of the defendants were charged with the "plunder of money, watches and other valuable property belonging to persons detained at the Celebici camp."[62] As part of the judgment, the Court determined that "it must be established that the prohibition of plunder is a norm of customary international law which attracts individual criminal responsibility."[63] In so finding, the Court stated "the Trial Chamber is in no doubt that the prohibition on plunder is also firmly rooted in customary international law."[64]

2. Elements of the Current Rule Prohibiting Pillage

While national military manuals differ slightly on the clarity with which they define and prosecute pillage, some examples are helpful. The U.S. Manual for Courts-Martial makes it an offense for a member of the armed forces to "quite his place of duty to plunder or pillage" when "before or in the presence of the enemy."[65] The Canadian LOAC Manual states that "[p]illage is theft, and therefore is an offence under the Code of Service Discipline."[66]

Perhaps most importantly, both the International Criminal Tribunal for Yugoslavia ("ICTY") and the International Criminal Court ("ICC") have added clarity with respect to the individual elements of pillage for prosecution in their jurisdictions. In the *Jelisic* case, the ICTY described

---

60. *Id.* at art. 4.

61. ICRC Rule 52, *supra* note 11.

62. Prosecutor v. Delalić, IT-96-21-T, Judgment, ¶¶ 18, 28 (Int'l Crim. Trib. for the Former Yugoslavia Nov. 16, 1998).

63. *Id.*

64. *Id.*

65. In this context, the MCM defines pillage as "to seize or appropriate public or private property." Manual for Courts-Martial: United States (2019 Edition), JOINT SERV. COMM. ON MIL. JUST., at IV-34, ¶ 23.b.(2)(b), https://jsc.defense.gov/Portals/99/Documents/2019%20MCM%20(Final)%20(20190108).pdf?ver=2019-01-11-115724-610.

66. *See* ICRC Rule 52, *supra* note 11, at § A.

plunder as "the fraudulent appropriation of public or private funds belonging to the enemy or the opposing party perpetrated during an armed conflict and related thereto"[67] and accepted Jelisic's guilty plea based on his admissions that he "stole money, watches, jewellery [sic] and other valuables from the detainees upon their arrival at Luka camp by threatening those who did not hand over all their possessions with death."[68]

The ICC lists the elements of the war crime of pillaging in an international armed conflict as:

> 1. The perpetrator appropriated certain property.
>
> 2. The perpetrator intended to deprive the owner of the property and to appropriate it for private or personal use.
>
> 3. The appropriation was without the consent of the owner.
>
> 4. The conduct took place in the context of and was associated with an international armed conflict.
>
> 5. The perpetrator was aware of factual circumstances that established the existence of an armed conflict.[69]

Under the ICC statute, the elements of the war crime of pillaging in a non-international armed conflict are the same, except element 4 requires "[t]he conduct took place in the context of and was associated with an armed conflict not of an international character."[70] These elements have been applied in several cases[71] and will continue to play a key role in future trials.[72]

Assuming that these basic elements will continue to apply to future criminal trials, there are some key pieces of these elements that deserve more attention, particularly in anticipation of applying these elements to cyber activities discussed in Part III. The following paragraphs will analyze these key pieces.

a. Perpetrator

One of the key contrasts between the ICC elements and the definition as stated in some of the State military manuals is the ICC's use of the term

---

67. Prosecutor v. Jelisić, Case No. IT-95-10-T, Judgment, ¶ 48 (Int'l Crim. Trib. For the Former Yugoslavia Dec. 14, 1999).

68. *Id.* at ¶ 49.

69. ICC Elements of Crimes, Art. 8(2)(b)(xvi) (2011), https://www.icc-cpi.int/resourcelibrary/official-journal/elements-of-crimes.aspx#article8-2b-xvi.

70. *Id.*

71. *See* Prosecutor v. Katanga, ICC-01/04-02/12, Judgment, ¶ 903 (Dec. 18, 2012); *see also* Prosecutor v. Gombo, ICC-01/05-01/08, Judgment, ¶¶ 113-125 (Mar. 21, 2016).

72. ICC, Kony et al. Case, https://www.icc-cpi.int/uganda/kony (listing the alleged crimes of Joseph Kony)*; see* Prosecutor v. Kony, ICC-02/04-01/05.

"perpetrator" as opposed to a reference to members of an armed force generally or, as in the case of New Zealand, members of their own armed forces.[73]

The ICC's more general application of pillage to any perpetrator is an important expansion. It clearly continues to cover members of armed forces, both those belonging to states and those belonging to non-state actors such as transnational terrorists and criminal organization. However, historical precedent from World War II suggests that the term "perpetrator" could also refer to both non-state actors and entities,[74] as well as corporations.[75] Indeed, calls are increasing for this expanded responsibility under the doctrine of pillage.[76]

In addition to members of any armed forces, corporations, terrorist organizations, and other non-state actors, the State itself may also be held accountable for pillage carried out by its forces. Tuba Inal makes this clear, referring to Nobel Prize winner, Louis Renault, and his comments after the 1907 Hague Conventions, where Renault argued that one of the innovations of the Convention was to make a State party "subject to penalties and responsible for all acts committed by the members of its armed forces, [and] gave rise to international liability and removed all doubts about the compulsory character of the Statute."[77] Article 3 of the 1907 Conventions states, "[a] belligerent party which violates the provisions of the said Regulations shall, if the case demands, be liable to pay compensation. It shall be responsible for all acts committed by persons forming part of its armed forces." Inal argues that this clear addition from the 1899 version of the Hague convention is a "recognition of the fact that violation of these rules gives rise to international liability."[78] Though not criminal liability,

73. New Zealand LOAC Manual, *supra* note 13, at ¶ 11.2.9.

74. *See* Updated Statute of the ICTY, art. 3(e), https://www.icty.org/en/documents/statute-tribunal (allowing the prosecution of "persons"); Menzel v. List, 267 N.Y.S. 2d 804 (Sup. Ct. 1966) (holding "'the Centre for National Socialist Ideological and Educational Research" is an organ of the Nazi Party responsible for pillage).

75. In the aftermath of WWII, the Nuremberg military tribunal prosecuted German corporations for pillage of the territory occupied by German forces, as seen in the treatment of the Krupp and Farben case. U.S. v. Pohl, TWC, Vol. II, Opinion and Judgment and Sentencing, 958 (Nov. 3, 1947); U.S. v. Krauch (Farben Case), TWC Vol. 8, 1081 (July 30, 1948); U.S. v. Krupp (Krupp Case), TWC Vol. IX, Judgment, 1327 (Aug. 17, 1947); U.S. v. Flick, TWC Vol. VI, Judgement, 1187 (Dec. 22, 1947).

76. *See, e.g.*, Open Society Foundations, *Why Corporate Pillage is a War Crime*, (May, 2019), https://www.opensocietyfoundations.org/explainers/why-corporate-pillage-war-crime (calling for prosecution as war criminals any corporation that knowingly buy, sell, or trade in pillaged goods).

77. *See* INAL, *supra* note 3, at 28.

78. *See id.* at 28-29.

the assignment of pecuniary liability to the State for pillage accomplished by state actors will be especially important in Part III.

b. Personal or Private Use

The ICC element of "for private or personal use" is not utilized by the ICTY, but still remains an element of most state military manuals that define pillage. It also is remains part of the historical underpinnings of the current prohibition.[79]

For example, the allowance for lawful requisition of private property is not unconditional. In fact, Article 52 of both the 1899 Hague Convention and the 1907 Hague Regulations specify that the requisition of private property must be for the necessities/needs of the army of occupation.[80] This is followed in state military manuals.[81] Indeed, one of the key elements which distinguishes lawful seizure or requisition from pillage is the purpose for which the property is taken. Invading and occupying armies have the right, in compliance with strict rules on compensation, to seize and/or requisition property based on military necessity. As stated in the *Gombo* trial decision:

> footnote 62 of the Elements of Crimes, which specifies, with reference to the requirement that the perpetrator intended to appropriate the items for "private or personal use", that "[a]s indicated by the use of the term 'private or personal use', appropriations justified by military necessity cannot constitute the crime of pillaging."[82]

Takings for private or personal use being proscribed, the key point of distinction between lawful and unlawful takings, therefore, is the existence or absence of military necessity.

---

79. JOHN HENRY MERRYMAN, ALBERT E. ELSEN, AND STEPHEN K. URICE, LAW, ETHICS AND THE VISUAL ARTS 27 (4th ed. 2007) ("The principle based upon the Roman Law according to which property seized during a war is put on an equal footing with the property seized in the air, in the sea or in the earth, and which in a similar way becomes the property of the captor—since the right of war constitutes a just cause of acquisition—may be applicable to things liable or apt to be used for the needs of the army and belonging to the other belligerent. But it cannot be applied to private property which, if it has not become the object of requisition or sequestration, must be restored or compensated. The objects involved in the present case are private property which had not been requisitioned or sequestrated as it could not be used for the needs of the army. Their seizure must therefore be considered as having been effected by pillage.") (quoting the Venetian Court in *Mazzoni, as translated in*, ANNUAL DIGEST OF PUBLIC INTERNATIONAL LAW CASES 1927–1928, 564-565 (1931)).

80. *See* Convention (II), *supra* note 7; *see* Convention (IV), *supra* note 8.

81. *E.g.*, DOD LAW OF WAR MANUAL, *supra* note 4, at § 15.11.

82. Prosecutor v. Gombo, ICC-01/05-01/08, Judgment, ¶¶ 113-125 (Mar. 21, 2016).

c. Takings Without Consent

In order for a perpetrator to pillage, the taking must be without the consent of the owner of the property. The consent must be genuine, meaning not brought about by coercion or some other form of force. The Trial Court in *Gombo* explained that the lack of consent may be inferred from the facts.[83]

> Furthermore, in accordance with Article 30(3), the perpetrator must have been 'aware' of the fact that the property was appropriated without the consent of the owner. This is assessed in light of the general circumstances of the events and the entirety of the evidence presented. The Chamber considers that, in situations where the perpetrator appropriated property in the absence of the owner or in coercive circumstances, the perpetrator's knowledge of non-consent of the owners may be inferred.[84]

The victim's knowledge of the theft not being required for pillage to have occurred will be important in applying pillage to cyber activities in Part III.

d. Armed Conflict

Finally, for the charge of pillage under the LOAC, the taking must occur in the course of an armed conflict and the perpetrator must have knowledge of the armed conflict. As was previously discussed, common usage of the term "pillage" is not always confined to situations of armed conflict. However, as a historical matter, the crime of pillage could only occur during armed conflict, and international law continues to recognize the perpetrator's knowledge of the existence of armed conflict as an element of the crime.

C. *Conclusion to Part II*

Despite the current propensity for evolving the definition and applying pillage more broadly, as discussed in Part II(A), states continue to use a narrower definition in line with the elements outlined in Part II(B). Perhaps the most important aspect of this narrower definition is the limitation to armed conflict. States still require an armed conflict as a threshold determination before assessing either individual criminal responsibility or state responsibility. In light of this, Part III's application of pillage to cyber activities will draw from these elements, as states apply them.

83. Prosecutor v. Gombo, ICC-01/05-01/08, Judgment, ¶ 121 (Mar. 21, 2016).

84. *Id.*

III. CYBER PILLAGE

Given the definition of pillage as the non-consensual taking of public or private property by members of armed forces for private or personal use (noting that "armed forces" can include both state and non-state actors or other agents of a Party to a conflict), cyber pillage would be defined as such a taking by cyber means. As will be demonstrated below, many cyber actors are conducting a wide variety of action under various circumstances that might look like pillage. However, though many of these activities are harmful and often illegal under both international and domestic law, only a limited subset will qualify as cyber pillage. The following sections will apply the definitional elements of pillage to cyber actions and draw conclusions based on such analysis, including with respect to the impact of an evolved definition in line with current usage.

A. *Perpetrator*

As discussed above, the use of the term "perpetrator" is a purposeful expansion of who (or what) qualifies as an actor that can pillage. Though most states define pillage in terms of armed forces, it has been clear, at least since the 1907 Hague Convention, that other entities could also be perpetrators of pillage. This would include not only non-state actors, such as terrorist groups and transnational actors, but also individuals, corporations, and ultimately, even states. This entire breadth of actors is currently engaged in cyber activities that might meet the definitional elements of cyber pillage. The following sections will discuss these actors in detail.

1. Armed Forces

As history indicates, members of the armed forces are the traditional perpetrators of pillage. They are also the group universally agreed to be subject to the prohibition and to individual criminal liability for violation of the rule. Certainly, the armed forces of the state are precluded from engaging in cyber operations that amount to pillage. For example, soldiers who are members of the armed forces of an occupying power would absolutely be precluded from using cyber tools to steal intellectual property or trade secrets from civilian companies within the occupied territory and then sell those secrets for personal gain.

Similarly, members of other armed forces, including members of organized armed groups, that are Parties to the conflict would also be subject to the prohibition. This would be the case in both international

armed conflicts and non-international armed conflicts. In other words, all fighters in the armed conflict are prohibited from pillaging.

2. Terrorists and Transnational Criminal Groups

Terrorist organizations or transnational criminal groups that meet the requirements of being organized armed groups in an armed conflict would fall under the category listed above. However, terrorists or transnational criminal groups that do not meet this classification are also precluded from pillage in connection with an armed conflict. More will be said below concerning the importance of the nexus involving an armed conflict, but it is sufficient here to say that simply not being considered an "organized armed group" under the LOAC does not prevent a terrorist or a transnational criminal organization from being considered a perpetrator for the purposes of the elements of the crime of pillage.

The involvement of these groups in the cyber theft of IP and other items has contributed to the pressure on the traditional notion of pillage. However, under the ICC elements of pillage, these groups would certainly qualify as "perpetrators" for purposes of prosecution.

3. Individuals and Corporations

Individuals and corporations can pillage in the same way as armed forces or terrorists, simply by meeting the requirements as stated. For example, if a corporation provides services such as site security for military supplies in the area of armed conflict and decides to use cyber tools to redirect shipments of goods bound for a local business to its own supply points, the corporation would likely be in violation of the prohibition on pillage. Similarly, cyber actions by an individual who diverts resources or convertible goods from its rightful owner to another would mean that the individual meets the threshold qualification of pillage.

4. States

The use of cyber tools as a means of state craft is increasing at an astonishing rate. Numerous cyber events have been attributed to states over the past decade, many of which proved quite devastating, and some even resulting in death and destruction.[85] This has resulted in many states listing

85. Julie H. Davis, *Hacking of Government Computers Exposed 21.5 Million People*, N.Y. TIMES (Jul. 9, 2015), https://www.nytimes.com/2015/07/10/us/office-of-personnel-management-hackers-got-data-of-millions.html (describing the hacking of DoD's Classified network and OPM); Andy Greenberg, *The Untold Story of NotPetya, the Most Devastating Cyber Attack in History*, WEIRD (Aug. 22, 2018), https://www.wired.com/story/notpetya-cyberattack-ukraine-

cyber threats as among their top national security priorities.[86] It is absolutely clear that states are actively conducting cyber operations against both other states and other entities.

As a result of the increasing threat, several countries have created military commands focused on the application of cyber tools,[87] including the U.S.[88] The Commander of USCYBERCOM is tasked to "direct, synchronize, and coordinate cyberspace planning and operations to defend and advance national interests in collaboration with domestic and international partners."[89] Note that the mission includes both a defensive aspect and potentially an offensive aspect.

The U.S. Congress provided its sense of what it might mean to "advance national interests" in the 2019 National Defense Authorization Act when it stated:

---

russia-code-crashed-the-world/ (expounding Russia's Notpetya attack that was intended for Ukraine, but spread around the world cause more than $10 billion worth of damages); John Leyden, *Hack on Saudi Aramco Hit 30,000 Workstations, Oil Firm Admits First Hacktivist-Style Assault to Use Malware?*, REGISTER (Aug. 29, 2012), https://www.theregister.co.uk/2012/08/29/saudi_aramco_malware_attack_analysis/ (describing Iran's malware attack that turned 30,000 of Saudi Aramco's computers useless); Ellen Nakashima & Joby Warrick, *Stuxnet was Work of U.S. and Israeli Experts, Officials Say*, WASH. POST (Jun. 2, 2012), https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html (explaining U.S.'s use of Stuxnet to destroy nuclear centrifuges in Iran); David. E. Sanger & Nicole Perlroth, *U.S. Escalates Online Attacks on Russia's Power Grid*, N.Y. TIMES (Jun. 15, 2019), *https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html* (discussing U.S.'s hacking into Russia's power grid for their sabotaging of U.S. power plants, water supplies and other public necessities); Scott Shane & Mark Mazzetti, *The Plot to Subvert an Election: Unraveling the Russia Story so Far*, N.Y. TIMES (Sep. 20, 2018), https://www.nytimes.com/interactive/2018/09/20/us/politics/russia-interference-election-trump-clinton.html (reviewing Russia's known meddling in U.S. elections).

86. Peter Dutton, *Cybersecurity is a National Priority for Australia*, STRATEGIST (Nov. 18, 2019), https://www.aspistrategist.org.au/cybersecurity-is-a-national-priority-for-australia/; Zolan Kanno-Youngs, *Homeland Security Chief Cites Top Threat to U.S. (It's Not the Border)*, N.Y. TIMES (Mar. 18, 2019), https://www.nytimes.com/2019/03/18/us/politics/homeland-security-cyberthreats.html (explaining the U.S.' top concern is cyber threats); *National Security Threats*, CTR. FOR THE PROT. OF NAT'L INFRASTRUCTURE, https://www.cpni.gov.uk/national-security-threats (last visited Mar. 17, 2020) (listing Cyber security as one of the UK's top concerns).

87. Elias Chachak, *The Top 10 Countries Best Prepared Against Cyber Attacks*, CYBER RESEARCH DATABANK, https://www.cyberdb.co/top-10-countries-best-prepared-cyber-attacks/ (last visited Mar. 17, 2020) (listing the United States, Israel, Russia, Canada, United Kingdom, Malaysia, China, France, Sweden, and Estonia as the countries most prepared for cyberattacks); Donald J. Mihalek & Richard M. Frankel, *Cyberspace is the New Cold War: Analysis*, ABC NEWS (June 21, 2019), https://abcnews.go.com/US/cyberspace-cold-war-analysis/story?id=63872848.

88. JAMES M. INHOFE, NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2020, S. REP. NO. 116-48, at 155 (116th Sess. 2019).

89. U.S. CYBER COMMAND, https://www.cybercom.mil/About/Mission-and-Vision/ (last visited Mar. 23, 2020).

> It shall be the policy of the United States, with respect to matters pertaining to cyberspace, cybersecurity, and cyber warfare, that the United States should employ all instruments of national power, including the use of offensive cyber capabilities, to deter if possible, and respond to when necessary, all cyber attacks or other malicious cyber activities of foreign powers that target United States interests…[90]

This authority implicates both *jus ad bellum* and *jus in bello*, and makes it clear that Congress intends for cyber tools to be an important part of any future armed conflicts. In the course of employing such tools, the state could become liable for cyber pillage.

In addition to taking actions directly themselves, states have used proxies to conduct their operations. For example, it now seems clear that in 2007, Russia used Nahsi, a Russian youth organization, to conduct the cyber operations against Estonia.[91] These proxies can be guilty of pillage themselves, as discussed above. However, they can also implicate state responsibility. Articles 4, 5, 6, and 8 of the Articles on Responsibility of States for Internationally Wrongful Acts provide methods by which the actions of a non-state can be attributed to the state for the purposes of determining responsibility for wrongdoing.

Article 4[92] allocates state responsibility for *de jure* elements of the government and also *de facto* organs of the government, generally determined by checking for "complete dependence" by the non-state organization. [93] Article 8 also states that in cases of individuals or corporations that do not fit under Article 4, their actions can still be attributable to the state when the group or actor "is acting on the instructions of, or under the direction or control" of the state.[94] This is a very high standard to meet but is certainly possible in the cyber context.

Thus, a state that works through a proxy organization and provides significant assistance – that which amounts to more than simply providing training or supplies – and directs the day-to-day operations, can be liable, at least monetarily to victims of the pillage, since the actions of that organization can be attributed to the state.

---

90. National Defense Authorization Act for Fiscal Year 2020, § 394, 10 U.S.C. § 1636(a) (2019).

91. Juhan Tere, *The Financial Times: Kremlin-backed Group Behind Estonia Cyber Blitz*, BALTIC COURSE (Mar. 11, 2009), http://www.baltic-course.com/rus/_analytics/?doc=10962&ins_print.

92. *See* U.N. Secretary-General, *Report of the International Law Commission on the Work of Its Fifty-Third Session*, at 40, U.N. Doc. A/56/10-S/10 (Aug. 2004) [hereinafter ILC Report].

93. Case Concerning the Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosn. & Herz. v. Serb. & Montenegro), Judgment, 2007 I.C.J. 43, 205 (Feb. 27) (quoting Nicaragua v. U.S., Merits, Judgement, 1986 I.C.J. 14, at ¶ 110).

94. *Id.*

5. Conclusion to Part III(A)

The use of the term perpetrator by the ICC reflects a change to the law of pillage that states have not yet fully embraced, as states still mostly limit actors who can commit pillage to armed forces or other battlefield fighters. However, not only does the ICC reflect the views of at least Party States to the Treaty which formed the ICC itself, but also seems to take account of the increasing complexity of the modern battlefield. Under the ICC's statue, basically any person or entity could be a pillager and subject to some form of liability for actions that amount to pillage.

Additionally, this expanded definition recognizes the impact of the previous discussion on the more modern interpretation of cyber pillage. Allowing any perpetrator to commit the crime will hopefully increase not only criminally liability when deserved, but also act as a deterrent to those potentially contemplating the crime.

B. *Personal or Private Use*

Given the extremely broad category of "perpetrator" – basically anyone or any entity that can conduct cyber operations – the next element of the definition provides a significant limitation to the commission of pillage. Ultimately, the true gravamen of the offense of pillage is that the goods taken are put to personal or private use. As mentioned earlier, if used to support the army of occupation or if taken without consent but remunerated, the element of personal or private use is not achieved.

In addition to the normal limitation, this element is completely devoid of a cyber-specific additive, such as the taking of cyber tools like code, programs, and cyber infrastructure, including servers or computers, as well as other "cyber" tools for an authorized use, and the subsequent use of these tools in addition to that approved use. The making of unauthorized copies of digital tools and applying them to personal use should also meet the elements of cyber pillage.

For example, assume a soldier requisitions computer hardware to assist in running the occupation.[95] Such a requisition would be completely lawful if done in accordance with Articles 46 and 52 of the Hague Regulations.[96] However, assume that the soldier takes some of the requisitioned computer hardware and uses it to operate his private business. Of course, and as already stated, a soldier who uses cyber tools to steal intellectual property

95. Note that one of the authors was also a member of the Group of Experts that wrote the Tallinn Manual. *See* TALLINN MANUAL 2.0, *supra* note 40 (discussing the difficulty in determining the difference between public and private cyber property).

96. *Id*.

and convert it to the soldier's personal use would be in violation of the prohibition of pillage. This would be true even under the expanded definition of pillage in common usage.

C. *Taking Without Consent*

Pillage, by its definition, requires a taking. With tangible artifacts, such as precious metals, currency, artwork, and other objects that have historically been the subject of pillage, the definition may seem quite simple to discern. However, as discussed in the Tallinn Manual 2.0,[97] with respect to digital information or data, what constitutes a taking is not always an easy question.

Initially, the question of whether a cyber activity is a taking requires a classification of the property. As discussed in the Tallinn Manual:

> A distinction must be made between use of the terms 'confiscation' and 'requisition' in this Rule. The Occupying Power may 'confiscate' State movable property, including cyber property such as computers, computer systems, and other computing and memory devices, for use in military operations. Private property may not be confiscated. 'Requisition' by the Occupying Power is the taking of private goods or services with compensation. Such taking is only permissible for the administration of occupied territory or for the needs of the occupying forces, and then only if the requirements of the civilian population have been taken into account.[98]

This would include the requisition of cyber property.

In addition to the examples provided, digital property would also be subject to taking, such as computer software and other digital data. For example, the digital records of personnel that worked at a local private utility would presumably be subject to requisition in order to facilitate the administration of the utility. On the other hand, if those personnel records were sold by a soldier to a digital vendor, the act would constitute pillage.

When considering the expanding definition of pillage discussed in Part II(A), the massive theft of trade secrets and IP by a non-state actor would also count as a taking, even if only digital copies of data were stolen. However, the next requirement for criminal responsibility under the LOAC would preclude such takings from criminal liability in most circumstances.

---

97. *Id*.

98. *Id*. at 200.

D. *Armed Conflict*

Finally, criminal liability under international law for cyber pillage can only take place in the context of an armed conflict. In contrast, much of the cyber interaction between states as catalogued above has been in the context of *jus ad bellum*, and not armed conflict. Similarly, much of the cyber activity described as "cyber pillage" has taken place between private parties during times of peace. At least with respect to cyber pillage that leads to criminal liability under the LOAC, such activity can only take place in the context of an armed conflict.

Though not accounted for as the majority of cyber actions thus far, cyber tools have already played an important role in armed conflicts in Georgia,[99] Ukraine,[100] Israel,[101] and in the fight against ISIS.[102] Given the trend of states to prepare their militaries for cyber activities during armed conflict, it is almost certain that cyber activities will not be a part of every future armed conflict. Therefore, though the requirement of armed conflict works as a significant limitation to the common usage of the term, it certainly does not preclude future criminal prosecutions for cyber pillage.

E. *Conclusion to Part III*

Given the elements of pillage as announced by the International Criminal Court and the general acceptance of this restrictive view by states, it is only a narrow set of cyber actions that will lead to criminal responsibility. Despite the seemingly expanding definition of pillage, particularly as reflected by the newest edition of Black's Law Dictionary and opinions of commentators, states have not endorsed this view.

One of the most important reasons for states maintaining the narrow view of pillage is the potential consequences of taking a different approach,

---

99. John Markoff, *Before the Gunfire, Cyberattacks*, N.Y. TIMES (Aug. 12, 2008), https://www.nytimes.com/2008/08/13/technology/13cyber.html.

100. Julian Coman, *On the Frontline of Europe's Forgotten War in Ukraine*, GUARDIAN (Nov. 12, 2017), https://www.theguardian.com/world/2017/nov/12/ukraine-on-the-front-line-of-europes-forgotten-war.

101. Erica D. Borghard & Jacquelyn Schneider, *Israel Responded to a Hamas Cyberattack with an Airstrike. That's Not Such a Big Deal*, WASH. POST (May 9, 2019), https://www.washingtonpost.com/politics/2019/05/09/israel-responded-hamas-cyberattack-with-an-airstrike-thats-big-deal/.

102. Zac Doffman, *New Cyber Warning: ISIS or Al-Qaeda Could Attack Using 'Dirty Bomb'*, FORBES (Sep. 13, 2019); https://www.forbes.com/sites/zakdoffman/2019/09/13/cyber-dirty-bomb-terrorist-threat-is-real-warns-us-cyber-general/#776196b9679f; David E. Sanger, *U.S. Cyberattacks Target ISIS in a New Line of Combat*, N. Y. TIMES (Apr. 24, 2016), https://www.nytimes.com/2016/04/25/us/politics/us-directs-cyberweapons-at-isis-for-first-time.html.

at least under international law. If states were to accept the most recent Black's definition, virtually all of the cyber actions catalogued in this article would amount to pillage and give rise to potential criminal liability under international law. Such a determination would also mean that each act of pillage under the expanded definition would amount to a violation of international law, allowing states to respond to such cyber actions with countermeasures.[103]

Countermeasures are otherwise illegal acts in response to an initial illegal act, but excused under international law when conducted in order to bring the offending state back into compliance with international law.[104] The acts must be tailored to the initial wrong, proportionate, reversible, and not amount to a use of force.[105] Countermeasures, which have been so narrowly tailored to limit such use, carries a real threat of escalation between states if utilized. Elevating the status of otherwise non-qualifying cyber actions under international law to an illegal act is simply a move that states currently seem unwilling to make.

Therefore, the current limitation of pillage to the elements as generally laid out by the ICC serves to contain the legal consequences of cyber activities in accordance with the current desires of states.

IV. CONCLUSION

The historical underpinnings of the crime of pillage continue to influence states when considering modern cyber activities. In continuing to adhere to the definition of pillage as the non-consensual taking of public or private property for private or personal use during armed conflict, states have elected to exclude a vast array of current cyber actions, conducted both by states and by non-state actors, from conduct that is illegal under the LOAC.

Instead, states limit cyber pillage to the taking of property for private or personal use in the context of an armed conflict. While this is a significant limitation, it still provides an important constraint on the activities of cyber actors during armed conflict, particularly in an age where cyber activities are becoming increasingly key to military operations.

---

103. ILC Report, *supra* note 92, at art. 22.

104. Denis Alland, *Countermeasures of General Interest*, 13 EUR. J. INT'L L. 1221, 1221 (2002).

105. ILC Report, *supra* note 92, at art. 49-54.