University of Michigan Journal of Law Reform

Volume 52 | Issue 4

2019

Different Problems Require Different Solutions: How Air Warfare Norms Should Inform IHL Targeting Law Reform & Cyber Warfare

Christian H. Robertson II
University of Michigan Law School

DIFFERENT PROBLEMS REQUIRE DIFFERENT SOLUTIONS: HOW AIR WARFARE NORMS SHOULD INFORM IHL TARGETING LAW REFORM & CYBER WARFARE

Christian H. Robertson II*

On February 19, 2018, United Nations Secretary-General Antonio Guterres claimed that he was "absolutely convinced" that "the next war will begin with a massive cyber-attack to destroy military capacity . . . and paralyze basic infrastructure." The Secretary-General's greatest concern, however, is that he believes "there is no regulatory scheme for that type of warfare, it is not clear how the Geneva Convention or international humanitarian law applies to it." Although Additional Protocol I to the Geneva Conventions (AP I) targeting laws generally identify who and what States may target in war, it expressly limits itself to attacks affecting people and objects on land. But what about online?

This Note discusses the limited applicability of the current targeting laws to cyber warfare. Specifically, it asks whether the land-centric AP I targeting laws adequately address cyber-attacks. It analogizes the unique features of cyber warfare to those in air warfare. Because both cyber and air warfare, unlike land combat, are fought beyond the traditional battlefield and closer to civilians, are object-prime targeting methods of warfare, and serve strategic attack objectives, AP I land-centric targeting laws cannot adequately regulate these types of warfare. This Note finds that, like airspace, the cyberspace domain is sufficiently different from land and, thus, requires specific rules similar to those provided under the laws of air warfare.

TABLE OF CONTENTS

* J.D., May 2018, University of Michigan Law School. To the memory of an extraordinary pilot, mentor, and dear friend, Lt. Col. Steve "Shooter" Eadie, who served his country with grit and dedication. Although no longer with us, his call for excellence and insatiable curiosity continues to inspire. Rest assured, brother, for life's unanswered questions: I don't know, but I'm fascinated to find out. Cheers, Shooter.

INTRODUCTION

On February 19, 2018, United Nations (UN) Secretary-General Antonio Guterres spoke at the University of Lisbon about a growing concern that has perplexed both States and international humanitarian law (IHL) academics for the greater part of the twenty-first century: the threat of cyber warfare. "I am absolutely convinced that, differently from the great battles of the past, which opened with a barrage of artillery or aerial bombardment, the next war will begin with a massive cyber-attack to destroy military capacity . . . and paralyze basic infrastructure."[1] Secretary-General Guterres' concern, however, is not the use of cyberspace in war but rather the *inadequacy* of current IHL to address it. "What is worse

1. Andrei Khalip, *U.N. Chief Urges Global Rules for Cyber Warfare*, REUTERS (Feb. 19, 2018), https://www.reuters.com/article/us-un-guterres-cyber/u-n-chief-urges-global-rules-for-cyber-warfare-idUSKCN1G31Q4.

[than the potential harm caused by cyber operations] is that there is no regulatory scheme for that type of warfare, it is not clear how the Geneva Convention or international humanitarian law applies to it."[2] While many agree with the Secretary-General's prediction that cyber warfare will play a significant role in future conflicts, some—like the International Group of Experts who published their interpretation of the existing international law's applicability to cyber operations and warfare in the Tallinn Manuals 1.0 and 2.0—argue that the laws of war found generally within the Geneva Conventions and specifically within the Additional Protocol I to the Geneva Conventions of 1949 (AP I) more than adequately cover cyber warfare.[3] While general rules and concepts of AP I might readily apply to cyberspace, the laws of targeting are land-centric.[4] How do the laws of land warfare address cyber-attacks and why should the international community endeavor for them to do so?

This Note discusses the applicability of the current AP I targeting laws to cyber warfare. Specifically, it asks whether the land-centric AP I targeting laws adequately address cyber-attacks. By reviewing the AP I *travaux préparatoires* and its subsequent interpretation, this Note finds that the cyberspace domain is sufficiently different from land and, thus, requires specific rules similar to those provided under the laws of air and naval warfare. First, in Part I, the Note identifies the current IHL shortcomings and provides examples illustrating them. Part II relates the current cyber issue to unique aspects of air warfare that resulted in targeting laws distinct from those in land warfare. Part III then highlights the unique characteristics of cyber warfare and the inability of AP I targeting laws to address them. Having identified a need for specific cyber warfare targeting laws, Part IV introduces new norms and rules for the international community to adopt and discusses policy considerations.

---

2. *Id.*

3. TALLINN MANUAL ON INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (Michael N. Schmitt ed., 2013) [hereinafter TALLINN MANUAL 1.0]; TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS (Michael N. Schmitt ed., 2d ed. 2017) [hereinafter TALLINN MANUAL 2.0].

4. Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts, art. 49, § 3, June 8, 1977, 1125 U.N.T.S. 17512 (entered into force Dec. 7, 1978) [hereinafter Additional Protocol I], https://treaties.un.org/doc/Publication/UNTS/Volume%201125/volume-1125-I-17512-English.pdf.

I. TALLINN APPROACH & CYBER QUESTIONS

According to some, the current IHL regime sufficiently addresses cyber warfare. "Despite the novelty of cyber operations and the absence of specific rules within the law of armed conflict explicitly dealing with them, the [Tallinn] International Group of Experts was unanimous in finding that the law of armed conflict applies to such activities during both international and non-international armed conflicts . . . ."[5] The twenty international law experts who gathered in Tallinn, Estonia in 2013 and again in 2017 claimed that cyber warfare did not operate beyond the reaches of IHL in a "legal vacuum."[6] Under this Tallinn approach, IHL covers cyber warfare. But what do IHL targeting laws actually say about cyber warfare?

Since 1977, Articles 48-56 of AP I have articulated the general laws of targeting. There, States incorporated the three fundamental targeting rules: distinction, necessity, and proportionality. First, Article 48 sets forth the rule of distinction. It provides that "[p]arties to a conflict shall at all times *distinguish* between the civilian population and combatants and between civilian objects and military objectives . . . ."[7] Through distinction arises civilian immunity that prohibits States from making civilians "the object of *attack*."[8] Article 49(1) defines "attacks" as "acts of violence against the adversary, whether in offence or in defence."[9] Like civilians and civilian populations, AP I protects "civilian *objects*" from being the "object of attack" resulting in "damage."[10] This would include anything that did not serve a military purpose, such as noncombatant homes or commercial buildings like a restaurant or mall.

Second, the AP I targeting laws describe the proportionality principle, which prohibits States from causing excessive collateral or incidental injury or damage. Specifically, Article 51(5)(b) prohibits States from attacking when such an "*attack* may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated."[11] "In case of doubt whether a person is a civilian"[12] and not

---

5. TALLINN MANUAL 2.0, *supra* note 3, at 375.
6. *Id.* at 378.
7. Additional Protocol I, *supra* note 4, art. 48 (emphasis added).
8. *Id.* art. 51, § 2 (emphasis added).
9. *Id.* art. 49, § 1.
10. *Id.* art. 51, §5(b), art. 52, § 1 (emphasis added).
11. *Id.* art. 51, § 5(b) (emphasis added).
12. *Id.* art. 50, § 1.

a combatant or "whether an object which is normally dedicated to civilian purposes . . . makes an effective contribution to military action,"[13] a presumption of immunity is required.

Third, like distinction and proportionality, the principle of necessity narrows permissible targeting. AP I strictly limits "attacks" to "military objectives."[14] Article 52(2) prohibits attacks that do not "offer[] a definite military advantage."[15] In essence, States may not attack people or objects unless it is necessary and they avoid causing unnecessary suffering.

These three principles—distinction, proportionality, and necessity—have become custom and apply generally throughout IHL to all methods of warfare. However, under AP I, States provided a specific caveat over these principles that is uniquely and solely applicable to attacks on land-based objectives:[16]

> The provisions of this Section apply to any land, air or sea warfare which may affect the civilian population, individual civilians or civilian objects *on land*. They further apply to all attacks from the sea or from the air against *objectives on land but do not otherwise affect the rules of international law applicable in armed conflict at sea or in the air.*[17]

AP I is limited in certain means of warfare. Article 49(3) expressly restricts the targeting laws enumerated under AP I to warfare affecting land and excludes from its reach targeting laws in other domains such as air and sea. How, then, do the AP I targeting laws apply to cyber warfare? How do the Tallinn experts assert that the cyberspace square peg fits in the AP I round hole? To better understand the issue, several scenarios illustrate the shortcomings under AP I targeting laws as applied to cyber warfare.

> *Scenario 1*: In a war between State A and State B, State A's cyber forces hack into the databases of a major oil exporter in State B and tamper with communications processing functions thereby disrupting its shipping data. This disrupts state revenue necessary to sustain State B's war effort. However, State A causes no physical damage to the exporter's personnel or property.

---

13. *Id.* art. 52, § 3.
14. *Id.* art. 52, § 2.
15. *Id.*
16. *Id.* art. 49, § 3.
17. *Id.* (emphasis added).

> *Scenario 2*: During the same war, State B's cyber forces upload a virus to a major private bank in State A, and the virus deletes millions of bank accounts owned by State A citizens that the bank controlled. Consequently, for weeks, millions of State A citizens are unable to access funds held by or credit accessed through the victim bank.
> *Scenario 3*: In response to State B's cyber operation, State A's cyber forces direct a denial of service (DOS) operation against a computer-based control system of an electrical distribution grid in a remote State B town that primarily supports commercial mining operations but is located near a military air defense station. The operation causes the control system to stop functioning, but it causes no physical damage to the hardware.

In contrast to the International Group of Experts' argument, it is unclear how AP I target laws would apply to these scenarios. How do AP I targeting laws apply to States A and B's cyber operations—that is, how does the Tallinn approach answer these cyber questions? Do AP I targeting laws even govern cyber warfare conducted on a solely virtual domain, beyond its land-centric limits under Article 49(3)? Would cyber tampering with communication processing functions, deleting bank account data, or DOS operations against control systems constitute "attacks" or "acts of violence" as defined in AP I? Do communication processing functions, bank account data, or computer-based control systems online constitute "civilians," "civilian populations," or "civilian objects" that are immune from such cyber operations? Does AP I regulate a DOS operation that does not cause "violence" or "property damage"? Can AP I targeting laws limit cyber operations against computer systems that have both civilian and military uses?

This Note argues that the current targeting law regime under AP I is insufficient because it fails to address targeting issues unique to cyberspace or, at least, it leaves these cyber questions up to expansive interpretation. Certainly, general IHL principles apply and cyber warfare does not completely operate in vacuum. However, IHL currently fails to address certain aggressive behavior unique to cyber warfare—as illustrated above—that the international community should prohibit. While targeting principles of distinction, proportionality, and necessity apply generally to all methods of warfare, the international community should strive to define parameters specific to the cyber domain as it has under AP I for land warfare. Otherwise, States will increasingly develop and employ

devastating cyber tactics and techniques with little-to-no regard for IHL targeting laws.

States are not unaccustomed to reforming IHL in response to new means of warfare. Air warfare—barely a century old—challenged the international community's understanding of targeting laws and, as the next Part explains, States agreed on new rules. Much like the international community's efforts to reform air warfare targeting laws, States should unite to reform targeting laws that are specific to cyber warfare. When new means of warfare develop, new rules are often required. Different problems require different solutions.

II. LESSONS FROM AIR WARFARE & IHL TARGETING LAW REFORM

Like cyber warfare, the rapid development of air power changed how States fought war and challenged the laws of land warfare. Just over a century ago, States revolutionized warfare by introducing air power on a major scale. As air power developed, the laws of war were slow to keep up. These developments in the law of air warfare arose out of the shortcomings of traditional land-centric laws. As air power rapidly developed into the twentieth century, States realized that they could not outright prohibit its use in war as attempted in the First Hague Convention, nor could they regulate it under the laws of land warfare. States would come to learn that the significant differences between air and land warfare necessitate different regimes of targeting laws. Problems unique to air warfare required different solutions.

A. *The Hague Rules of Air Warfare & New Protection for Civilians*

Since the invention of the hot air balloon by Joseph and Etienne Montgolfier in 1783, States have looked for ways to use air power in war. After episodes of balloon warfare in the nineteenth century, States agreed to prohibit military balloons from launching projectiles and explosives under the First Hague Peace Convention of 1899.[18] Under this regime, States viewed hot air balloons as an extension of land warfare and regulated them accordingly.

Up until the nineteenth century, land warfare was largely limited to the battlefronts. There, armies seldom encountered non-

18. Declaration to Prohibit, for the Term of Five Years, the Launching of Projectiles and Explosives from Balloons, and Other Methods of Similar Nature, July 29, 1899, 32 Stat. 1839.

combatants and, thus, land warfare laws did not expressly provide protection for "civilian populations" or "civilian objects" prior to the Geneva Conventions.[19] Instead, Article 25 of the Hague Convention only prohibited forces from attacking or bombarding "towns, villages, dwellings or buildings which [were] *undefended*. . . ."[20] Additionally, armies had different incentives to protect non-combatants as occupying forces than air forces or navies had. Specifically, armies historically tried to avoid conflict with local citizens to maintain order.[21] Granting these non-combatants strict immunity from armed attack was one way of achieving such order.[22] These rules and incentives were specific, however, to the strategies and traditions of land warfare. Their applicability to air warfare was short-lived.

Shortly after the outbreak of World War I in 1914, forces quickly introduced air power to the fight. States did not limit their use of air power to the battlefronts, though. Instead, they also flew missions behind enemy lines and, for the first time in history, attacked civilians and non-combatants in the heart of enemy territory without having breached the front lines of the battlefield. Germany used its air forces to bombard London while France conducted air raids on Karlsruhe and Stuttgart.[23] As both sides continued their air assault, they ironically accused each other of violating Article 25 of the Hague Convention. Germany claimed that France violated the law against attacking undefended towns because towns like Karlsruhe were non-fortified towns, far from the battlefront, and therefore, illegitimate targets.[24] Meanwhile, Britain argued that bombing London had no military purpose and was thus an illegitimate target.[25] Despite their accusations, neither the Allies nor Germany could justify their attacks under the protection of the "undefended towns" standard set forth under the Hague Convention.

After the war, nations gathered at the Washington Conference of 1922 to re-evaluate the laws of air warfare. There, a Commission concluded that the Hague Convention of 1907 could not ade-

---

19. Amanda Alexander, *The Genesis of the Civilian*. 20 LEIDEN J. OF INT'L L. 359, 365 (2007).

20. Convention Respecting the Laws and Customs of War on Land, art. 25, Oct. 18, 1907, 36 Stat. 2277 (emphasis added).

21. Jeremy Rabkin & Ariel Rabkin, *Navigating Conflicts in Cyberspace: Legal Lessons from the History of War at Sea*, 14 CHI. J. INT'L L. 197, 203 (2014).

22. *See id.*

23. J.M. SPAIGHT, AIR POWER AND WAR RIGHTS 200–02 (1924).

24. *Id.*

25. M.W. ROYSE, AERIAL BOMBARDMENT AND THE INTERNATIONAL REGULATION OF WARFARE 179 (1928).

quately regulate all aspects of air warfare.[26] Because States found air power appealing, air power was an inevitable means of warfare that the laws of war had to address.[27] The appeal of air power was that it allowed States to conduct effective offensive attacks by air while keeping its attacking forces—i.e. pilots—beyond the reach of enemy defenses.[28]

After deliberation at the Washington Conference, the Commission drafted the Hague Rules on Air Warfare of 1923.[29] Accepting air power as a legitimate method of warfare, the Commission found that its differences from land warfare necessitated special treatment under the laws of war.[30] Among the critiques of the old laws, academic contemporaries highlighted the inadequacy of the "undefended towns" standard to provide warring States with clear aerial targeting guidance as among the most significant. They found that the standard was untenable because of the inherent differences between air warfare and land warfare.[31] Specifically, air warfare differs from land warfare in that it (1) operates beyond the boundaries of the traditional battlefield, (2) primarily targets objects instead of persons, thus, complicating distinction principles, and (3) serves an attack objective to reduce the adversary's ability to wage war unlike land attacks that seek to capture and occupy land.[32]

---

26. *See* James W. Garner, *Proposed Rules for the Regulation of Aerial Warfare*, 18 AM. J. INT'L L. 56, 65 (1924).

27. *See id.* ("[T]he very potency of the airship as an instrument of destruction in war is such that there is no reason to believe that states will ever totally renounce the employment of it as an arm of combat, and restrict its use to services of exploration, observation and communication . . . . Any such proposal [for such rules prohibiting air warfare] must be regarded as purely chimerical.").

28. *See generally id.* (recognizing the risk reduction that pilots in World War I experienced compared to soldiers. Unlike land warfare that had to advance either through or around enemy forces, aircraft could fly over battlefields and bomb enemy targets with less resistance).

29. Hague Rules of Air Warfare (1923), https://wwi.lib.byu.edu/index.php/The_Hague_Rules_of_Air_Warfare. *See also Rules Concerning the Control of Wireless Telegraphy in Time of War and Air Warfare. Drafted by a Commission of Jurists at the Hague, December 1922 - February 1923*, INTERNATIONAL COMMITTEE OF THE RED CROSS, https://ihl-databases.icrc.org/ihl/INTRO/275?OpenDocument (last visited Apr. 14, 2019).

30. *See* Garner, *supra* note 26, at 81 ("Considering the role which aircraft seems destined to play in the wars of the future and the frightful consequences which its unregulated use will produce, and considering both the paucity and inadequacy of the existing conventional rules, the recommendations to the Commission of Jurists deserve the urgent and serious consideration of the governments to which they are addressed.").

31. *See id.* at 57.

32. *See id.* at 70.

1. Unique Air Domain: Closer to Civilians & Farther from the Battlefield

The first difference the Commission's academic contemporaries noted between air and land warfare was the difference in combat locations.[33] Unlike land warfare fought on countryside battlefields, air campaigns took place closer to civilians and far above land forces. The Commission's contemporaries recognized the enhanced mobility and reach that air power had and the problematic application of the geographically limited Hague Convention targeting laws.[34] As States began targeting military-supporting industries deep behind enemy lines, targeting rules tied to the presence of troops or the proximity to the battlefield became unworkable. "Land fighting is less mobile and shifting [than air warfare]; it is more localised geographically and the zone in which it can be regarded as existing is normally a fairly well-defined one."[35] Alternatively, "aircraft carry . . . their own zones of operations with them . . . . They create their battle zones as they go."[36]

The Commission's contemporaries realized that, with air power, States now had the ability to overcome land limitations and bypass land force resistance.[37] Air power enabled States to quickly penetrate enemy territories and reach civilian locales. For air forces, the operating environment is often in a more civilian-centric area, unlike land forces who historically fought battles away from populated areas. Moreover, the "undefended towns" standard is a land force concept. The standard was determined by the presence of land forces or lack thereof. Specifically, the terms "defended" and "undefended" related to the location of land forces that created the battlefield. Contemporary academics believed that the operation of air power beyond the battlefield—unlike ground forces who formed it—required a re-evaluation of targeting rules.[38]

2. Air Warfare's Object-Prime Target Type

The Commission's contemporaries also argued that air warfare requires a different governing regime because air forces primarily target buildings on the ground or aircraft in the sky, as opposed to

---

33. *See* SPAIGHT, *supra* note 23, 198–201 (comparing British, French, German, and Italian air attack practices).
34. *See id.* at 203–05.
35. *Id.* at 205.
36. *Id.*
37. *See* Garner, *supra* note 26, at 64.
38. *See id.* at 70.

people.[39] In other words, air warfare has an object-prime target type. While land forces primarily target soldiers—that is, people—air forces most often attack objects. The difference is significant for targeting laws in applying the distinction principle.

As discussed earlier, States may not target indiscriminately. Distinguishing between threatening and non-threatening objects in the vast skies is comparatively more difficult than identifying combatants on the battlefields.[40] "[T]he danger of surprise on the part of apparently inoffensive civil aircraft will probably impose upon the latter (enemy civil aircraft) special restraints as the price of immunity."[41]

The Commission addressed the distinction issue resulting from air power's object-prime targeting nature by reducing immunity protections generally afforded to civil aircraft. Specifically, the Hague Rules of Air Warfare removed the "undefended town" standard. The Commission's contemporaries concluded that the term "defended" referred to the fortification of towns by sentries or armies.[42] In other words, it is a combatant-prime targeting rule. Because attacking armies could readily identify opposing ground forces—such as sentinels patrolling a town or armies barricading a village—the undefended town standard was a feasible targeting approach for land warfare. It was largely ineffective for air forces, though, because air power primarily targets objects. From thousands of feet in the air, pilots were unable to determine whether a town was defended by people on the ground. Moreover, air defense was a relatively novel tactic that States did not formally deploy during World War I. Accordingly, the unique nature of air warfare required a new standard.

3. Air Attack Strategic Objective to Reduce War Waging Ability

A third major critique of applying land-centric targeting laws to air warfare was the inapplicability of the "undefended town" standard to aerial combat. According to the Commission's academic contemporaries, the term "defended" under the Hague Convention related directly to the military purpose of land forces: to capture and occupy land.[43] In other words, a town was only "defended" or "undefended" when forces capable of inducing its surrender

---

39. *See* SPAIGHT, *supra* note 23, at 205, 217.
40. *See id.* at 217.
41. 2 L. Oppenheim, International Law 309, 530 (H. Lauterpacht, 7th ed. 1952).
42. *See* SPAIGHT, *supra* note 23, at 213-14.
43. *See* Garner, *supra* note 26, at 70.

and occupation confronted it. This was not the objective of air forces. Instead, States deployed air warfare to "simply destroy the place or certain person or things in it."[44]

The Commission's contemporaries believed—as many do today—that air power serves a more strategic role of reducing an adversary's ability to wage war by, among other things, crippling its infrastructure or reducing its military industrial output.[45] Flying thousands of feet above targets without the objective or ability to capture and occupy towns, air warfare rendered the "undefended town" standard inapplicable.[46] The Commission's contemporaries found that "[t]he distinction between 'defended' and 'undefended' places as a test of liability to bombardment is reasonable enough in land and naval warfare, but when applied to aerial bombardment it is illogical and even absurd."[47] Because air warfare did not seek to capture or occupy towns like land forces did, the Commission's contemporaries concluded that the "undefended town" standard did not apply and, therefore, certain aspects of air warfare required different targeting laws.[48]

4. New Air Warfare Targeting Rules

These differences between air and land warfare led to IHL reform. After the Washington Conference, the Commission drafted and proposed the Hague Rules of Air Warfare. This set of rules included two significant changes. First, Article 14(1) introduced the distinction between military objectives and civilian objects:

> Aerial bombardment is legitimate only when directed at a military objective, that is to say, an object of which the destruction or injury would constitute a distinct military advantage to the belligerent.[49]

Second, Article 14(4) made air bombardment of "cities, towns, villages . . . or buildings" legitimate provided that they were "in the immediate neighborhood of the operation of land forces" and with "regard to the danger thus caused to the civilian population."[50]

---

44. *Id.*
45. *See id.*
46. *Id.*
47. *Id.*
48. *See id.* at 70-72.
49. Hague Rules of Air Warfare, *supra* note 29, art. 14, § 1.
50. *Id.* at § 4.

These two concepts reformed targeting rules as they applied to air power. The international community recognized air power's unique operating environment closer to civilians and behind enemy lines, its distinction issues, and its strategic purpose of targeting its adversary's military infrastructure or industrial output.

Due to the different nature of air warfare, prior land targeting laws failed and required change. In World War I, States like Britain and Germany abused the "undefended towns" standard of protection and launched air assaults on cities far behind the fronts. Aware that air power was not going away, States reformed the rules and created the Hague Rules of Air Warfare. Instead of applying old solutions to new problems, the Washington Commission identified key differences between the then-existing laws and the new effects of air warfare.

B. *AP I & the Limited Regulation of Air Warfare Targeting Laws*

Although the Hague Rules of Air Warfare never became a treaty, States eventually memorialized their revolutionary features in AP I. Due to the increasing concerns created by air—as opposed to land—warfare, the international community convened to create AP I. "[T]he principal area of concern which motivated the initiatives that led to [AP I] . . . was a shared need to formulate more effective rules to protect the civilian population and individual civilians from the effects of attacks in light of the development of *air power*."[51]

The drafters of AP I noted that "air power vastly extended the depth of the ground battle areas" beyond those seen in land warfare.[52] While the drafters noted the significance of air power's reach into enemy territory, States were more concerned with targeting laws applicable to effects on land and objected to creating one, all-encompassing targeting law.[53] "[C]ountries with substantial navies who believed it would be dangerous to attempt a revision of existing treaty and customary law on . . . attacks of enemy merchant ships" strongly resisted an all-encompassing targeting law.[54]

---

51. *See* BOTHE ET AL., NEW RULES FOR VICTIMS OF ARMED CONFLICTS: COMMENTARY ON THE TWO 1997 PROTOCOLS ADDITIONAL TO THE GENEVA CONVENTIONS OF 1949, at 315 (2d ed. 2013) (emphasis added).

52. *Id.*

53. *See* CLAUDE PILLOUD ET AL., INT'L COMM. OF THE RED CROSS, COMMENTARY ON THE ADDITIONAL PROTOCOLS OF 8 JUNE 1977 TO THE GENEVA CONVENTIONS OF 12 AUGUST 1949, at 634 (Yves Sandos et al. eds., 1987).

54. *See* BOTHE ET AL., *supra* note 51, at 331.

During negotiations, some States believed that land warfare laws could regulate air warfare because of its connection to land, namely its air-to-ground bombing function. The majority of States, however, emphasized that air warfare also operates in two other domains: at sea and in air. These distinct functions of air persuaded States to refrain from broadly applying AP I targeting laws to all air operations. In response to the land effect concerns, States agreed to limit the applicability of AP I targeting laws to attacks "on land" and exclude air-to-air operations as well as naval combat solely at sea.[55]

C. *Air-to-Air Targeting Laws Under the Air & Missile Warfare Manual*

As discussed, AP I art. 49(3) expressly limits its applicability to warfare targeting civilians, civilian populations, and civilian objects *on land*. Because States found air warfare so uniquely different from land, they left one of the primary functions of air power outside the scope of AP I: air-to-air combat. This carveout has resulted in different targeting laws for air-to-air combat. Specifically, under the Manual of Air & Missile Warfare ("AMW Manual"), air-to-air targeting rules have fewer restrictions on attacking enemy civilian aircraft than AP I has on targeting civilians on land.[56] Much like the Washington Commission had recognized years before, States made this distinction because of the inherent differences between air and land combat.[57]

The AMW drafters agreed with the Commission's understanding of the air domain as uniquely distinct from land and created air attack rules for targeting civilian objects that were more lenient than land-based rules.[58] Additionally, States like the United States and United Kingdom have maintained the difference in objectives be-

---

55. *See id.*; *see also* Additional Protocol I, *supra* note 4, art. 49, § 3.

56. *See generally* PROGRAM ON HUMANITARIAN POLICY AND CONFLICT RESEARCH AT HARVARD UNIVERSITY, HPCR MANUAL ON INTERNATIONAL LAW APPLICABLE TO AIR AND MISSILE WARFARE (2013) (revealing that, for example, the AMW Manual permits combat aircraft to attack other aircraft normally dedicated to civilian purposes if the pilot has reasonable grounds to believe that the aircraft has become a military objective. Conversely, AP I presumes that unidentified objects or persons are not lawful targets when the attacking combatant is in doubt).

57. MARCO SASSOLÍ ET AL., *Air Warfare*, *in* HOW DOES LAW PROTECT IN WAR?, INT'L COMM. OF THE RED CROSS, https://casebook.icrc.org/law/air-warfare#_ftnref_020 (commenting on the AMW Manual by stating that the "[r]ules for attacks on targets on land which specify them, must be 'proved by reference to the peculiar conditions of air warfare.' In this respect, the Manual on Air and Missile Warfare helps identify in what respect the details must be adapted to the physical realities of the air environment.").

58. *See id.*

tween air and land attacks.[59] Specifically, they define the objectives of air force strategic attack to be reducing their adversary's ability to wage war rather than capturing and occupying land.[60]

As apparent from the AMW Manual, air-to-air combat has required different targeting laws. For reasons unique to air power, such as its domain beyond the battlefield, its object-prime targeting, and its strategic attack objective, AP I targeting laws are not applicable to air-to-air combat. States and international law experts should not seek to place domain-specific targeting laws on other methods of warfare. Like airspace, cyberspace has significant differences from land warfare. Thus, warfare conducted solely online or within the cyber domain should have different targeting laws that adequately address the unique problems it presents.

III. NEW PROBLEMS IN CYBER WARFARE

Just as air power extended the effects of war to the skies and beyond the traditional battlefield, cyber capabilities similarly bring new challenges distinct from those inherent in land warfare. Nevertheless, some States and experts like the Tallinn Group continue to assume the laws of war under AP I targeting law sufficiently cover cyber operations much as States did for air power before 1923. However, like air power, cyber warfare operates beyond the boundaries of the traditional battlefield, primarily targets objects instead of people, and serves attack objectives to reduce the adversary's ability to wage war unlike land attacks that seek to capture and occupy towns. These similar features should inform the international community's process of rethinking cyber warfare targeting laws. Specifically, States should rethink cyber targeting laws and (1) distinguish cyber operations beyond the domain of AP I, (2) define "objects" protected from the cyber warfare, and (3) identify what constitutes a "cyber-attack."

---

59. *Compare* SECRETARY OF THE AIR FORCE, AIR FORCE DOCTRINE DOCUMENT 3-70 (2011) [hereinafter AFDD 3-70], https://fas.org/irp/doddir/usaf/afdd3-70.pdf (describing the objective of a "Strategic (Air) Attack" as "to weaken [the] adversary's ability or will to engage in conflict."), *with* MINISTRY OF DEFENSE, JOINT DOCTRINE PUBLICATION 0-30 (2d ed. 2017) (U.K.) [hereinafter MINISTRY OF DEFENSE PUBLICATION 0-30], https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/668710/doctrine_uk_air_space_power_jdp_0_30.pdf (defining "Strategic (Air) Attack" as an "[attack] aimed at an adversary's fundamental ability to wage war, by attacking their structures or organisations" and claiming that "[t]argets may include centres of gravity, such as leadership and command elements, critical war production resources or key supporting infrastructure.").

60. *See* AFDD 3-70, *supra* note 59, at 49; MINISTRY OF DEFENSE PUBLICATION 0-30, *supra* note 59, at 33.

A. *The Cyberspace Domain Beyond AP I but Closer to Civilians*

Like air warfare, Article 49(3) excludes the applicability of AP I targeting laws to certain attacks within cyberspace. As discussed above, AP I targeting laws only apply to "warfare which may affect the civilian population, individual civilians or civilian objects on land" and not to attacks conducted in other domains.[61] It is unclear, however, whether certain cyber operations "affect [targets] on land" such that AP I applies. To resolve this issue, States and academics alike have sought to define "cyberspace." However, even if cyberspace requires a different definition, one must then ask why it should receive different targeting laws. That, like the deep penetration of air forces beyond the battlefront in World War I, is because cyberspace is much closer in proximity to civilians than the traditional battlefield and, thus, requires a different analysis.

1. Defining Cyberspace Beyond the Land Battlefield

According to the Tallinn experts, cyberspace is "[t]he environment formed by physical and non-physical components to store, modify, and exchange data using computer networks."[62] Under the Tallinn definition, a portion of cyber operations—those formed by the "non-physical" components—escape AP I's regulation. Unlike "physical" components such as computers, servers, or other land-based objects, "non-physical storage, modification, and exchange" of digital data occurs in a virtual domain online. For air warfare, the international community understood that it could have effects on land and, therefore, it included of air-to-ground attacks under the targeting laws of AP I. At the same time, States recognized operations that occurred solely outside the land domain such as the air-to-air combat discussed earlier or, perhaps, operations that occur through the non-physical components of cyberspace. Rejecting universal AP I targeting laws, States removed air-to-air from its reach. Similarly, operations through the non-physical component of cyberspace—that is, "cyber-to-cyber"—are beyond the specific targeting norms set forth under AP I.

The United States defines cyberspace as more distinct from other domains than the Tallinn experts do. The United States Department of Defense Law of War Manual defines "cyberspace" as a "global domain within the information environment consisting of interdependent networks of information technology infrastruc-

---

61. Additional Protocol I, *supra* note 4, art. 49, § 3.
62. TALLINN MANUAL 2.0, *supra* note 3, at 564.

tures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[63] The significance of the U.S. definition is that it clearly separates cyber-attacks from existing domains of war. The United States distinguishes the "global domain" as "a new domain of warfare" separate from "land, sea, air, and space."[64] Under the U.S. definition, cyber operations operate largely in a new domain, beyond the traditional battlefield, with problems inherently different from those addressed under AP I's targeting laws.

2. Cyberspace in Closer Proximity to Civilians

The understanding of the cyber domain has varied amongst academics. Some argue that the cyber/land distinctions are irrelevant under the AP I so-called "Martens Clause"[65] and the International Court of Justice (ICJ) opinion in *Nuclear Weapons*.[66] Under the Martens Clause, proponents of AP I argue that IHL's failure to expressly prohibit warfare that subjects civilians and combatants to violence against "custom[,] . . . the principles of humanity and . . . the dictates of public conscience" are nevertheless regulated by the general principles of IHL.[67] The ICJ upheld the effectiveness of Martens Clause in its *Nuclear Weapons* Advisory Opinion. There, the Court held that the Martens Clause was "an effective means of addressing the rapid evolution of military technology" involved in nuclear warfare.[68]

Accordingly, many argue that cyber is merely a new weapon that AP I covers as prescribed under the Martens Clause and as understood in *Nuclear Weapons*. The problem, however, is not the existence of generally applicable targeting rules under IHL—such as distinction, proportionality, and necessity—but the lack of specific rules that encourage compliance. Professor Marco Roscini claims that "[t]he problem with the extension of existing rules and principles to new scenarios such as cyber operations is that they do not take into account their uniqueness and might prove to be too gen-

---

63. U.S. DEPARTMENT OF DEFENSE, LAW OF WAR MANUAL para. 16.1.1, at 1012 (2015) (citing Joint Chiefs of Staff, Joint Pub. 3-12: Cyberspace Operations, at GL-4, (Feb. 5, 2013)).

64. *Id.* at 1012 n.3 (citing William J. Lynn III, Deputy Secretary of Defense, *Defending a New Domain: The Pentagon's Cyberstrategy*, 89 FOREIGN AFFAIRS 97, 101 (Sept./Oct. 2010)).

65. INT'L COMM. OF THE RED CROSS, INTERNATIONAL HUMANITARIAN LAW AND THE CHALLENGES OF CONTEMPORARY CONFLICTS 47 n.52 (2015).

66. *See id.* at 40.

67. Additional Protocol I, *supra* note 4, art. 1, § 2.

68. Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 104, ¶ 78 (July 8, 1996).

eral" for States to follow.[69] When States seek to graft old, general rules onto new, specific problems, there are both intentional and practical concerns regarding compliance. First, some States might intentionally abuse AP I targeting laws as they would be applied to cyber because the laws are overly general. Second, and perhaps the greater concern, is that many States willing to comply will be unable to because AP I's vagueness as applied to cyber would deprive them of any practical guidance.

As the land-centric "undefended towns" standard during air campaigns in World War I proved to be impractical for air warfare, current AP I targeting laws will likely prove to be too general within the cyberspace domain. Like air warfare, and unlike land warfare, cyber operations are conducted in close proximity to civilians. According to studies gathered by Professor Robin Geiss, "approximately 98 per cent of US government communications use civilian-owned and operated networks."[70] Cyber warfare is closer to civilians than any form of warfare has ever been. Unless States reform targeting laws to adapt to cyber warfare beyond AP I, there will likely not be a deployable understanding of what constitutes an "object" protected from cyber operations and whether those operations even amount to an "attack" regulated by IHL.

Through similarities in the Tallinn and U.S. definitions in cyberspace, this Note argues that cyber operations conducted in the "global domain within the information environment consisting of interdependent networks of information technology" through "non-physical components to store, modify, and exchange data" fall outside the specific rules of AP I targeting laws. Under this assertion, all the cyber operations illustrated in Scenarios 1-3 in Part II would likely fall outside the scope of specific targeting laws in AP I. State A could claim that tampering with an oil exporter's communications processing functions online occurs on a "non-physical component" of data exchange and storage. State B might similarly argue that deleting bank account data does not reach the "physical component" that triggers land warfare targeting laws. State A might have the weakest claim under Scenario 3: that its DOS operation is beyond the scope of AP I because of the effects its operation had on an electrical grid control system. State A might, nevertheless, assert that the control system is an online, virtual function that does operate in the physical sense. Even if its claim is unpersuasive, the unclear nature of AP I art. 49(3) would make it diffi-

---

69. MARCO ROSCINI, CYBER OPERATIONS AND THE USE OF FORCE IN INTERNATIONAL LAW 23 (Oxford Univ. Press 2014).

70. Robin Geiss & Henning Lahmann, *Cyber Warfare: Applying the Principle of Distinction in an Interconnected Space*, 45 ISRAEL L REV. 381, 386 (2012).

cult for State B to condemn the cyber operation. Finally, notwithstanding the domain issues, even if we assume these cyber operations fall within the AP I purview, AP I targeting laws do not adequately address these scenarios.

B. *Civilian Intangible Property & Regulated "Objects"*

AP I art. 52 regulates attacks on civilian "objects", but what constitutes an "object"?[71] Does its meaning even matter when Article 52(3) limits attacks to objects which by their "nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction . . . offers a definite military advantage"?[72] Under the ICRC's understanding, and even that of the Tallinn experts, the meaning of "object" matters. According to the ICRC's Commentary to AP I, "objects" under AP I refers only to "visible and tangible" things.[73] Pursuant to the ICRC Commentary, the Tallinn experts concluded that "[d]ata is intangible and therefore neither falls within the 'ordinary meaning' of the term object, nor comports with the explanation of it offered by the ICRC."[74]

What does this limitation mean for cyber warfare? States, arguably, have greater targeting options with respect to data than any other target. The Tallinn experts define "data" as "[t]he basic element that can be processed or produced by a computer to convey information . . . the fundamental digital data measurement is a byte."[75] Data would include processing functions, programming language, command algorithms, and mere informational data.

This understanding of protected "objects" provides States A and B with significant interpretive latitude in Part II Scenarios 1-3. For State A in Scenario 1, the oil exporter's online communications processing might not be an "object" safe from attacks. There, State B might have a strong argument that the processing is operated through its tangible computer hardware; however, if the communications processing is only a series of command functions it likely would not constitute an "object." The same analysis would likely apply to State A's cyber operations against the electrical grid control system in Scenario 3, although State B's "object" claim would likely be more persuasive because of the significant infrastructure

---

71. Additional Protocol I, *supra* note 4, art. 52.
72. *Id.* at § 2.
73. PILLOUD ET AL., *supra* note 53.
74. TALLINN MANUAL 2.0, *supra* note 3, at 437.
75. *Id.* at 564.

involved in an electrical grid. On the other end of the spectrum, State B's targeting of State A's bank accounts in Scenario 2 would likely constitute intangible objects not protected under AP I. As Secretary-General Guterres feared, cyber operations targeting these types of data are likely vulnerable under the AP I shortcomings.

C. *Cyber Operations Short of "Attacks"*

AP I art. 49(1) defines "attacks" as "acts of violence against the adversary."[76] Like the term "object", does the meaning of "attacks" limit the scope of AP I targeting laws in cyber warfare? Is denying software processing or deleting online data an "attack"? There are two primary issues with the meaning of "attack" in cyber warfare: first, the focus on means (force applied) or ends (resulting harm) and second, whether loss of use or function without damage or injury even amounts to an attack.

1. Cyber-Attacks Determined by Force Applied or Resulting Harm

Under the Commentary to AP I, the commentators explained that the word "attacks" "applies to those aspects of military operations which most directly affect the *safety* of the civilian population and the *integrity* of civilian objects."[77] The objectives of "safety" and "integrity" coincide respectively with the protections from "injury to civilians" and "damage to civilian objects" under Article 51(5)(b).[78] Under the Commentary explanation, "attacks" and "acts of violence" prohibited "denote[] physical force."[79] Moreover, and perhaps most significant to the understanding of cyber-attacks, the Commentary to AP I explained that "the concept of 'attacks' does not include . . . *non-physical means* of psychological, political, or economic warfare."[80] In light of the AP I Commentary, AP I-regulated "attacks" appears to limit its meaning to physical means of warfare.

The Tallinn experts disagree with this means-based definition of "attacks." Instead, the experts claimed that the "consequential

---

76. Additional Protocol I, *supra* note 4, art. 49, § 1.
77. BOTHE ET AL., *supra* note 51, at 328 (emphasis added).
78. Additional Protocol I, *supra* note 4, art. 51, § 5(b).
79. BOTHE ET AL., *supra* note 51, at 329.
80. *Id.* (emphasis added).

harm" bears more on the understanding of an attack.[81] To support their assertion, the experts cite, first, the international community's recognition of non-kinetic chemical, biological, and radiological operations as attacks and, second, the consequence-based focus throughout the AP I targeting laws.

First, the experts cite the International Criminal Tribunal of Former Yugoslavia's (ICTY) interpretation of chemical attacks in *Prosecutor v. Tadic*.[82] There, the court found that chemical operations constitute "attacks" under AP I even if they do not usually have a kinetic effect on their designated target.[83] States, however, might easily distinguish cyber operations from chemical attacks by contending that no harm befell any person or tangible property. Unlike chemicals that have injurious effects on the human body and the natural environment, a cyber DOS operation generally does neither unless it reasonably led to consequences that physically manifested.

The Tallinn experts' second effects-based argument cites the AP I language that focuses primarily on the consequences of "attacks" that the targeting laws seek to protect rather than focusing on the force applied.[84] Specifically, the proportionality principle expressed under Article 51(5)(b) speaks of "*loss* of civilian life, *injury* to civilians, *damage* to civilian objects, or a combination thereof."[85] While strongly supported by the international community, this understanding of the term "attacks" does not appear to address non-physical consequences to intangible objects. It might, nevertheless, regulate cyber operations that States might reasonably expect to result in such physical harm.

This "reasonable expectations of harm" understanding of "attacks" is based in text and logic. Under AP I art. 56, "[w]orks or installations containing dangerous forces, namely dams, dykes and nuclear electrical generating stations, shall not be made the object of attack, even when these objects are military objectives."[86] This categorical restriction on targeting dams, dykes, and nuclear electrical generating stations supports the Tallinn experts' assessment of "attacks." In other words, if the attacking State launches cyber operations against a dam control-system—which is critical to preventing flooding—the consequential injury to persons or damage

---

81. TALLINN MANUAL 2.0, *supra* note 3, at 416.

82. Prosecutor v. Tadić, Case No. IT-94-1-ar72, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction (Int'l Crim. Trib. for the Former Yugoslavia Oct. 2, 1995).

83. *Id.*

84. TALLINN MANUAL 2.0, *supra* note 3, at 416.

85. Additional Protocol I, *supra* note 4, art. 51, § 5(b) (emphasis added).

86. *Id.* at art. 56, § 1.

to property would indicate an attack occurred. While AP I might adequately cover this aspect of cyber warfare, it still fails to regulate those that do not target such prohibited works and installations. For example, the reasonable expectations of harm test would not cover cyber-to-cyber operations targeting only data management industries. If a State launched a cyber operation against another State's banking industry, there would likely be no reasonable expectation of personal injury or physical damage. Although this operation will cause economic loss, it does not fit within the confines of AP I.

2. Cyber-Attacks & Loss of Use

The second question concerning cyber operations and attacks is whether an object's loss of use rather than damage or injury constitutes an attack. This is particularly relevant to the realm of cyber warfare because of the standard technique of DOS. A DOS operation is technically reversible and only temporarily renders the targeted system inoperable. Theoretically, there are three approaches to this question. First, and most limited, some might claim that cyber-attacks are limited to operations that cause violence to persons or physical damage to objects. Second, a cyber-attack occurs if the object targeted requires restoration to function again. Third, and most expansive, any operation that merely leaves an object without function constitutes an attack—that is, a type of functionality test.

Taken at face value, the text of Article 49(1) defining "attacks" strongly suggests that "violence" or physical injury or damage must occur. This appears to suggest the first and most limited approach discussed above. However, Article 52(2)'s discussion of attacks that result in target "neutralization"[87] supports the functionality test under the third approach. Under the Commentary to AP I, the word "neutralization," "insofar as it deals with bombardment, refers to an attack for the purpose of *denying* the use of an object to the enemy without necessarily destroying it."[88] To illustrate its meaning, the commentators provided an example where "enemy artillery or surface-to-air missiles may be *neutralized* for a sufficient time to prevent their interference with a planned operation by fir-

87. *Id.* at art. 52, § 2 ("Attacks shall be limited strictly to military objectives. In so far as objects are concerned, military objectives are limited to those objects which by their nature, location, purpose or use 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.").

88. BOTHE ET AL., *supra* note 51, at 367 (emphasis added).

ing anti-personnel munition at such targets in attempt to force gun crews to take shelter."[89] States could argue both that the Commentary's explanation provides for a broader understanding of an "attack" that includes DOS operations and for a narrower understanding that excludes it. In the former instance, a State might cite the clear language of *denial* within the meaning of *neutralization* that clearly makes DOS an attack. Alternatively, States might understand—like the Commentary—the term "neutralization" as limited to instances "insofar as [they] deal[] with bombardment." The generality of the term denies States and the international system with a workable rule. Moreover, opponents of the "functional test" of attacks can argue that, because electronic jamming operations[90] typically do not constitute attacks, neither should DOS operations.[91]

AP I's use of the term "attacks" was likely limited to physical attacks on land. Having identified how AP I "attacks" resulting in "personal injury" or "physical damage" have limited application to cyber operations conducted virtually, it is easy to see how States might push the limits, disregard, or misunderstand AP I targeting laws in Scenarios 1-3 of Part II. In Scenario 1, State A's tampering with the oil exporter's communications processing functions likely does not rise to the "physical" violence in the means-based understanding nor does it likely result in "injury" or "damage." State B's virus in Scenario 2, however, might come closest to resembling a conventional attack. Deleting or erasing data is akin to destruction that AP I generally prohibits. In Scenario 3, State A's DOS operation arguably would not rise to the level of an attack. Under the loss of use or functionality test, an attack would have occurred. However, the Commentary to AP I qualifies "neutralization" to instances of "bombardment." Moreover, this DOS operation strongly resembles electronic jamming that does not result in an attack. Applying these Scenarios to the unique challenges of cyber warfare illustrates the need to rethink cyber-specific targeting laws. The international community should rethink the new problems that require new solutions.

---

89. *Id.* (emphasis added).

90. Electronic jamming, included under the broader category of electronic warfare, involves the deliberate radiation or reflection of electromagnetic energy for the purpose of disrupting enemy use of electronic devices or systems, such as radio signals or radar.

91. INT'L COMM. OF THE RED CROSS, *supra* note 65, at 41–42.

IV. RETHINKING CYBER WARFARE TARGETING LAW NORMS

Cyber warfare is simply different from land warfare. Its domain and operating environment, primary target, and attack objectives are different from those for which States created AP I targeting laws. History has shown us how targeting laws are domain-specific and fail to adequately cover certain aspects of other means of warfare such as air combat. If target issues arise based on the method's primary target, then different targeting laws should apply. When States recognized the objective of air power to reduce the adversary's ability to wage war instead of capturing and occupying land, they re-evaluated the land-centric targeting laws under the Hague Convention. Similarly, States must recognize that the objective of cyber warfare is not to capture and occupy territory but rather to harass, deny, or degrade an adversary's virtual capabilities. To the extent that cyber-attacks do not manifest themselves in physical damage or personal injury, AP I is insufficient and States should create specific cyber targeting rules.

A. *Defining Cyberspace Domain*

One of the greatest issues with cyber warfare is the lack of existing definitions. Unlike other areas of IHL, cyber warfare is mostly theoretical and, therefore, unfamiliar to the world. As highlighted throughout this Note, States and non-state actors alike have varying understandings of what cyberspace is. Moreover, methods of warfare often have multiple sides with different treatment. As presented, AP I governs air-to-ground attacks but not air-to-air attacks.[92] A proper definition of cyberspace should include, as the Tallinn experts express, a "physical" and "non-physical" component. Like air and naval warfare, cyber operations can have effects on land—that is, vis-à-vis its physical component. This definitional point is significant to the clear application of AP I targeting rules to the cyber-attacks that result in injury of civilians or damage to objects. Additionally, the definition should explicitly invoke AP I targeting laws to cover the physical components of cyberspace. This would include physical components such as hardware, servers, terminals, land-lines, etc.

Politically, the advantages start with clarity. States have largely operated and developed cyber capabilities without clear guidance about permissible and impermissible targeting. By creating two

92. *See* Additional Protocol I, *supra* note 4, art. 49, § 3.

components—the physical and non-physical—States can not only develop specifically permissible targeting capabilities, but they can also focus cyber defense strategies. If the regime had two components, it would encourage States to invest in and implement relatively more aggressive counter-cyber defense systems that only operate within the non-physical component of cyberspace. In essence, these are systems built for cyber-to-cyber engagements. This will greatly reduce State vulnerabilities.

The disadvantage of this proposal is possibly creating a more lenient targeting standard for operations conducted in the non-physical component of cyberspace that States might abuse. Differing definitions would likely create different standards and, thus, incentives for States to opportunistically apply the one that fits their strategy. For instance, States might claim that they conduct all their cyber operations through the non-physical component to employ more devastating uses of cyber without committing acts of war. However, this aspect of differing standards is not new to States. As highlighted by AP I art. 49(3), means of air and naval warfare are governed by more lenient standards. For example, air combatants can use incendiary weapons in air combat, which are prohibited on land. Additionally, the broader targeting rights in air-to-air combat, as discussed in Part III, have not led to significant targeting law abuses.[93]

B. *Creating Protection for Essential Civilian Intangible Property*

AP I's focus on protecting "tangible and visible" civilian objects ignores an essential target of most cyber operations: data. Whether it is processing data, command functions, or substantive data, AP I targeting laws leave States and their civilian populations vulnerable. This is significant because intangible objects are the primary target of cyber-attacks. As air power is tangible object-prime, cyber operations is intangible object-prime. Data is the primary target, whether the aggressor seeks to deny its use or delete it altogether.

This Note proposes the inclusion of "essential civilian intangible objects" to the immunity list. Under this rule, "essential civilian intangible objects" would include "economic, political, and infrastructure data." This definition would protect the private sector and information essential to everyday life. States, both with large and small militaries, will have incentives to protect their economies and political organizations from cyber operations. This is in line

93. *See* SASSOLÍ ET AL., *supra* note 57.

with the distinction principle accepted more than a century ago. The issue, however, might be that the definition of "objects" goes too far such that the definition could immunize civilian objects historically subject to lawful attack when serving both military objectives. For instance, States could argue that certain intangible items like the media are protected even though they use it to coordinate military communications. States should, nevertheless, be able to overcome this concern by applying the military necessity principle to objectives permissible in cyber warfare.

Additionally, this immunity, along with the general scope of this Note, should be limited to *jus in bello* targeting laws. Essential civilian intangible objects targeted in commercial hacking or other cyber operations short of war are not protected under this rule. Instead, there, the *jus ad bellum* laws on "attacks" control.

C. *Expressly Adopting the "Functional" Approach to the "Attack" Definition*

The definition of "attacks" under a cyber warfare targeting law regime should expressly include the functional approach—or loss of use—and formally adopt the Tallinn Experts' understanding of neutralization. States should expressly adopt this definition for cyber targeting laws because, contrary to the Tallinn experts' claim, AP I targeting laws do not clearly extend to temporary and reversible functional losses. States created AP I targeting laws to address "loss of life" and "physical damage" of then-existing warfare. Unlike both land and air warfare, however, DOS and other neutralizing attacks are likely to be the norm rather than the exception in cyber warfare. Because such denials can also consequently result in serious works or installation damages, neutralization is more dangerous in cyber warfare and, thus, should be regulated as an attack.

D. *Application to Cyber Issues*

Under this new regime, each of the cyber operation Scenarios would be regulated. In State A's tampering with the oil exporter's communications processing systems, such tampering would be a "functional" attack that the proposed targeting law reforms would limit. State B's deletion of the private bank accounts would be an impermissible attack on "essential civilian intangible objects." Finally, State A's DOS attack on the electrical grid control system

would likely be a "functional" attack that is governed by the proposed regime.

While concerns might arise that these targeting rules cover more than they should, it will likely be to the benefit of States with advanced militaries for cyber targeting laws to cover more. States with advanced militaries tend to have relatively advanced economies. Today, those economies rely upon data security and civilian confidence in the markets in order to operate. These advanced economic States will likely want to protect aspects of their economy that they rely upon to a stronger extent than will developing States. Similarly, cyber capabilities today have somewhat leveled the playing field. Individuals in less advanced States can now attack aspects of powerful States' infrastructures by simply uploading a virus. Accordingly, advanced States are comparatively more vulnerable to attacks on data. They should be more willing to accept the comparatively lesser risk of new cyber targeting rules' over-coverage over the serious economic risk to their cyber-dependent industries.

CONCLUSION

For years now States and academics both have convened to discuss cyber warfare under international law. As is the case in many international law initiatives, different political and economic interests discourage States from creating significant changes. In the face of inertia, groups such as the Tallinn experts nobly seek to fill the legal voids by claiming that existing law covers the current problem. Although this approach eliminates any "legal vacuum" in which new problems might operate, it renders the solution too general to effectively govern the nuances of modern warfare. States and academics must still strive to create rules in war that eliminate unnecessary suffering. This Note does not advocate, however, that States seek all-encompassing definitions of or absolute bans on certain acts of cyber warfare. The legal pendulum should not swing to the other extreme and become so specific that it rarely applies. Instead, this Note suggests a new approach for States to take when considering cyber warfare laws. To adequately understand both the need to have cyber targeting laws and to have a set distinct from AP I's land warfare laws, States should consider cyber warfare's unique domain, primary targets, and attack objectives as they did for air warfare.

After World War I, J.M. Spaight claimed that air warfare was unique and required special rules to properly govern it. "It now remains to show why it is better to proceed by creating a new and special code . . . rather than by building upon and adding to the

rules already governing land warfare."[94] Instead of resting on the international law agreements of the past, Spaight understood that air warfare was inevitable, and that States should squarely address it rather than succumb to inertia. Like air power, cyber has unique characteristics that the current land-centric AP I cannot fully regulate. States have an incentive to define and limit cyber operations before cyber warfare targets State economies, infrastructure, and political institutions on a full scale.

Like air power, cyber operations operate beyond the boundaries of the traditional battlefield, primarily target objects instead of persons, and serve attack objectives to reduce the adversary's ability to wage war unlike land attacks that seek to capture and occupy towns. Because of these material differences between land and cyberspace, new rules are required to define the domain, protect essential civilian intangible objects, and identify the nature of "cyber-attacks" to be regulated.

94. *Spaight, supra* note 23, at 31.