PANEL 3
Paradigms & Policy: Proxies, Partners, & More

China and the Rule of Law: A Cautionary Tale for the International Community

by Maj. Ronald T. P. Alcala, Lt. Col. Eugene (John) Gregory and Lt. Col. Shane Reeves

June 28, 2018

The Communist Party of China has been leading an extraordinary effort to transform the country into a *fazhi* (法制) nation or "a country under the rule of law." The phrase "*fazhi*" has become ubiquitous in China, where it is heralded in all forms of media, from simple banners and posters, to pop-up ads on the internet. In fact, China has become so enamored with *fazhi* the Party dedicated an entire session of the 18th Party Congress to the subject in 2014. We should be cautious of accepting China's endorsement of the "rule of law" at face value, however. China's notion of *fazhi*—and its conception of law more generally—differs substantially from how rule of law is universally understood. Recognizing how China's cost-benefit approach to law erodes international norms and institutions should serve as a reminder that a stable, cooperative, rules-based international order requires a commitment to the restraining power of the law.

In a 2004 report on Rule of Law and Transitional Justice, the UN Secretary General observed that central to the rule of law is the requirement that the State itself is accountable to laws that are publicly promulgated, equally enforced and independently adjudicated. Other common characteristics of a nation under the rule of law include adherence to the principles of "supremacy of law, equality before the law, accountability to the law, fairness in the application of the law, separation of powers, participation in decision-making, legal certainty, and avoidance of arbitrariness and procedural and legal transparency." Ultimately, rule of law requires that State power itself must be subordinate and accountable to—that is, restrained by—the law.

China's recent commitment to the "rule of law" has produced some admirable results. Its emphasis on legality in the past 20 years has generated a considerable body of sophisticated, high quality legislation. Meanwhile, an explosion in legal education—as

measured by the increase in credentialed lawyers—has cultivated an impressive bar of domestic and international legal experts, while rapid construction of China's legal infrastructure, to include courthouses and procuratorate (or prosecutors') offices, has continued at an unprecedented pace. Indeed, Chinese President Xi Jinping has been so supportive of these developments that he established an annual Constitution Day highlighting the importance of law and the Constitution in establishing *fazhi*. Then, for the first time in Party history, he swore an oath to the Constitution, just like the leader of a rule of law nation would.

Despite the Party's current encouragement of "rule of law" and its celebration of the Constitution, Chinese rule of law—officially called "socialist rule of law with Chinese characteristics"—differs fundamentally from rule of law as internationally understood. To begin with, all aspiring Chinese lawyers—at least according to the study material for one bar exam preparation course—must commit to the belief that law is subject to the "leadership of the Party." The same bar review material further states that the fundamental principle of Chinese rule of law is to "maintain the rule of the Party." Meanwhile, a recent bar exam question affirmed that "Western Capitalist Rule of Law Thought" is not an "origin" of Chinese rule of law. Accordingly, rather than promote basic principles such as the supremacy of law, legal accountability, judicial independence, and fair treatment before the law, *fazhi* is instead used as a rhetorical tool to legitimize the Party's rule. It is the Party's will restated in seemingly neutral and distinctly legal language, which draws on a long imperial tradition of legal discourse while rejecting norms of transparency and impartiality. By evoking *fazhi*, the Party seeks to attain greater credibility, and in turn inspire greater compliance, by drawing on both the high prestige accorded to rule of law and the Chinese tradition of obedience to edicts of the ruler and the precedents of the dynasty (*qianli* 前例).

It is not surprising, then, that despite the Chairman's apparent enthusiasm for the Chinese Constitution, Chinese judges are still prohibited from citing the Constitution as a source of law. The Party smartly does not want to open that Pandora's Box; doing so could wreak havoc on the Party. The heady days of *Qi Yuling versus Chen Xiaoqi*, decided in 2001, when the People's Supreme Court cited the Constitution for the first time and seemed to signal a "sprout" of true Constitutionalism in China, are long over. While the Party wants "rule of law"—in the sense of an abundance of published law recognized and followed by the people—the highest levels of the Party do not want to be subject to the law or have the Party's will ever be challenged by the law. This is a tall order as the Party

needs the system to cast a wide and credible legal net (*fawang huihui* 法网恢恢) without creating the potential to ensnare the Party itself. Moreover, the Party needs the law to give the appearance of objective impartiality while simultaneously and reliably addressing cases that are of concern to the Party. More bluntly, the Party wants the credibility of impartial and independent law without the political danger.

To successfully navigate these competing interests, the Chinese legal system has become both increasingly routine (often impartial at the case-adjudication level), yet also highly and efficiently responsive to the will of the Party. This emphasis on routine impartiality lends some credibility to the claim that China is transforming into a rule of law nation. Yet ultimately, the Chinese legal system remains an instrument of the Party. This is why it is possible for a petty criminal in Beijing's Xindian District to receive a fair trial (as one of the authors observed two years ago) while a disgraced politician like Bo Xilai may be subjected to a show-trial. The Party's current rule of law campaign sincerely and energetically seeks to promulgate laws and to compel the Chinese people to follow the law—or, as the Chinese saying goes, "to have law to follow" and to "follow the law that exists." However, while adherence to *fazhi* may resemble a commitment to ideals such as legal accountability, legal certainty, and equality before the law, in fact "law" in China is a rhetorical restatement of the Party's discretionary will using legal discourse. This should not be mistaken for rule of law as the animating (or constraining) force is not the supreme authority of law, but the will of the Party.

Moreover, structural social differences, including what Lawrence Friedman described as internal and external legal cultures, help differentiate China from a nation under the rule of law. While the structure of Chinese and Western law is relatively comparable—legislators, law enforcement, trial and appellate courts, lawyers, judges, plaintiffs, bar associations—the internal legal culture (attitudes and practices of legal professionals) of China supports Party supremacy rather than actual rule of law. Transgressions of the law by the Party, therefore, regularly go unremarked and unaddressed. For example, it would never occur to a Chinese judge to issue an injunction against an order from Xi—and even if he wanted to, the judge would realize that the external legal culture (attitudes of the general population) in China would not support his decision either.

While legal scholars need not object to China's internal conception and application of law, they may rightly object to the Chinese appropriation of the term "rule of law" to describe what it is doing. At the very least, it is important to understand how China's

pragmatic use of law, and its refusal to be restrained by inconvenient law, correlates internationally, particularly as China uses its newfound wealth to demand a greater role in international rule-making and adjudication. Ultimately, it should not be taken for granted that China's obeisance to international institutions and legal norms—like its acknowledgment of "rule of law" domestically—reflects a genuine commitment to international law. Each instance of compliance—even large-scale routine compliance—is a cost-benefit exercise for the Chinese.

Although domestic law in China almost never openly conflicts with the Party's will, the Party's ability to bend international law to its will is far more restricted. Consequently, China has embraced international law and institutions when they can be used to advance its interests and has ferociously denounced them when they have not. Admittedly, this approach to international legal norms is merely pragmatic, and many States, including the United States, commonly engage in similar behavior. However, while States understandably interpret and apply international legal norms in ways that promote their national interests, China is conceptually incapable of viewing international law—with its collection of constraints and obligations—with the same deference as the rules-based international community. China simply does not believe that law by nature of its unique normative position has the power to constrain the will of the Party itself, either domestically or internationally, and this view is supported by both China's internal and external legal cultures. China may comply with certain international norms that conflict with its national interest, not out of a respect for the rule of law, but rather as part of a pragmatic cost-benefit analysis.

China's establishment of an Air Defense Identification Zone (ADIZ) in the East China Sea provides one example of China's acceptance and use of an international legal norm to advance its national interests. ADIZs were historically employed to deconflict air traffic and protect coastal states from unwanted intrusions into their sovereign airspace. Rather than use the East China Sea ADIZ to protect its sovereign airspace, however, China instead employs the ADIZ to assert sovereignty over the disputed Senkaku Islands. As one commentator described it, China's "extraterritorial layering of sovereignty rights reverses the underlying rationale of ADIZ from defensive to offensive, from the protection of national sovereignty to the coercive extension of sovereignty beyond territorial limits." Nevertheless, China readily adopted the ADIZ because it served a purpose consistent with the will of the Party. Moreover, it cast the Party's will in a rules-based, safety-oriented international legal norm.

In contrast, China vehemently denounced the 2016 arbitral award in the *South China Sea Arbitration* because it conflicted with its national interests and the will of the Party. Established pursuant to Annex VII of the 1982 UN Law of the Sea Convention (UNCLOS), to which China is a signatory, the arbitral tribunal rejected China's claim to sovereign rights or jurisdiction over marine areas within China's self-proclaimed "nine-dash line" in the South China Sea. Notably, China refused to accept the arbitral tribunal's jurisdiction from the start, arguing that the essence of the arbitration was "territorial sovereignty," which was "beyond the scope of the Convention," and did not concern "the interpretation or application of the Convention." The arbitral tribunal, however, held that it did have jurisdiction over almost all of the Philippines' submissions and noted that despite China's non-appearance at its proceedings, "China remains a Party to these proceedings, with the ensuing rights and obligations, including that it will be bound by any decision of the Tribunal." Moreover, under UNCLOS, the international legal basis for arbitration and the effect of an award are clear: The award of an arbitral tribunal "shall be final and without appeal" and "shall be complied with by the parties to the dispute."

China's response to the arbitral award, however, was dismissive. After first denouncing the Philippines' "unilateral initiation of arbitration" (Article 1, Annex VII of UNCLOS provides that "any party to a dispute may submit the dispute to the arbitral procedure") without first seeking to settle the dispute through negotiation (the arbitral tribunal found the Philippines "did seek to negotiate with China"), the statement then proceeds to repudiate not only the award but the tribunal itself. The statement asserts that the award is "null and void" and of "no binding force," and declares that "China neither accepts nor recognizes it." More ominously, the statement then attacks the integrity of the arbitral tribunal, claiming that its conduct and award "completely deviate from the object and purpose of UNCLOS," "substantially impair the integrity and authority of UNCLOS," and are "unjust and unlawful."

China's fierce reaction should not be surprising. In China, the Party can never violate the law because the Party's will is the law. Similarly, an international decision that conflicts with the Party's will is not merely wrong, but actually illegitimate. Meanwhile, an open assessment of China's compliance with legal norms is not possible in Chinese society because the Party controls the machinery of discourse. While the internal and external legal cultures of another State might have pushed back and debated the disparagement of an international legal body, in China the Party mobilized every venue of public discourse to vilify and delegitimize the decision. In fact, the moment the arbitral decision was

issued, the Chinese universally dismissed it as *naoju* (闹剧), literally a "noisy play" or "farce," indicating that putatively legal institutions, whether domestic or international—such as the arbitral tribunal—are only useful in so far as they comport with the Party's will. This approach is consistent with China's formal conception of the rule of law.

An effective rules-based international order requires that States accept the restraining power of the law. While China has acknowledged the importance of international law and observed legal norms when convenient, China's cost-benefit approach to legal compliance ultimately rejects the supremacy and power of law as a restraining force. This view derives from its own conception of law as an expression of the Party's will, nothing more. States that engage with China and those that consider China a reliable partner or fellow adjudicator in furthering the rules-based international order should understand its cost-benefit approach to the law and, consequently, how this influences its behavior. Of course, while undermining established norms and institutions when they frustrate perceived interests may weaken respect for the rule of law over time, from the Party's perspective it's simply a matter of perfecting *fazhi*.

The views expressed here are the authors' personal views and do not necessarily reflect those of the Department of Defense, the United States Army, the United States Military Academy, or any other department or agency of the United States Government.

Photo by China Photos/Getty Images

About the Author(s)

Maj. Ronald T. P. Alcala

Major in the U.S. Army; Assistant Professor in the Department of Law at the United States Military Academy, West Point, N.Y. Before joining the faculty, Major Alcala served as a Judge Advocate in a number of legal positions advising commanders on criminal law, international law, and administrative law issues.

Lt. Col. Eugene (John) Gregory

Lieutenant Colonel in the United States Army; Professor of Chinese in the Department of Foreign Languages at the United States Military Academy, West Point, N.Y.; Director of the Center for Languages, Cultures, and Regional Studies at the United States Military Academy.

Lt. Col. Shane Reeves

Lieutenant Colonel in the United States Army. He is an Associate Professor and the Deputy Head of the Department of Law at the United States Military Academy, West Point, New York (shane.reeves@usma.edu). The views expressed here are his personal views and do not necessarily reflect those of the Department of Defense, the United States Army, the United States Military Academy, or any other department or agency of the United States Government.

LAWFARE

INTERNATIONAL LAW: LOAC

Developing the Law of Armed Conflict 70 Years After the Geneva Conventions

By **Shane Reeves** Wednesday, August 7, 2019, 8:00 AM

The post below is the latest installment in Lawfare's *tradition of posting short pieces inspired by the annual Transatlantic Dialogues on International Law and Armed Conflict. This year, that event was organized and sponsored jointly by the Oxford Institute for Ethics, Law and Armed Conflict (directed by Dapo Akande), the South Texas College of Law (through the good offices of Geoff Corn), West Point's Lieber Institute for Law and Land Warfare (directed by LTC Shane Reeves), and the Robert Strauss Center for International Security and Law at the University of Texas (directed by* Lawfare's *Bobby Chesney).*

Recently the Lieber Institute for Law and Land Warfare at West Point, the Robert Strauss Center for International Security and Law at the University of Texas, the Oxford Institute for Ethics, Law and Armed Conflict, and the South Texas College of Law Houston co-sponsored the seventh annual Transatlantic Dialogues on International Law and Armed Conflict. This year's workshop took place 70 years after the adoption of the Geneva Conventions and provided a unique opportunity to reflect on the impact of these seminal treaties.

While there is no doubt the Geneva Conventions remain at the foundation of the law of armed conflict (LOAC), it is also clear that portions of these documents are difficult to reconcile with contemporary warfare. For example, Article 28 of the Geneva Convention Relative to the Treatment of Prisoners of War of August 12, 1949 (Geneva Convention III) discusses the details of operating a camp canteen, including types of items that must be available, pricing and how profits are used. Article 62 in the same convention notes that "[p]risoners of war shall be paid a fair working rate of pay by the detaining authorities direct. The rate shall be fixed by said authorities, but shall at no time be less than one-fourth of one Swiss franc for a full working day."

Obviously, it is difficult to find the above provisions relevant on the modern battlefield. Just as global militaries adapt doctrine, tactics and force structure to address battlefield realities, innovations in the law are necessary for effectual regulation. In other words, as the pace of change in military operations accelerates, the LOAC must also evolve or risk becoming detached from modern military realities.

Despite this necessity, new treaties are rare and customary international law is difficult to discern, as states are reticent to express concrete positions concerning the LOAC. As a result, the LOAC is glacial in adapting to the complexities of modern warfare, leaving numerous novel legal issues unaddressed.

With states generally silent, nongovernmental organizations (NGOs), expert drafted manuals and decisions of international tribunals are increasingly looked to for answers. This is logical, as these contributions are often quite valuable. Groups like the International Committee of the Red Cross (ICRC) are well versed in the LOAC and are persuasive in explaining how the law should be interpreted. Manuals, for their part, are important in helping state practitioners reach a common understanding on difficult legal topics while simultaneously stimulating dialogue. International tribunals, while ensuring LOAC compliance, offer critical explanations of how the law works in application.

Clearly, these efforts are extraordinarily important, especially as the baseline treaties underlying the LOAC age. But it is worth highlighting that states, despite their hesitancy, remain the creators of international law. NGOs, at most, indirectly influence state practice and are not empowered to develop the law. Many manuals, though often mistaken (albeit not by their drafters) as lex ferenda, are intended as restatements of the existing law intended to help state legal advisers. Finally, international courts and tribunals are limited by jurisdiction to only those states parties bound by the underlying promulgating treaty.

When states are unwilling to express their views about international law or are unable to come to bilateral or multilateral agreements, others fill this void. Humanitarian groups conduct widely publicized conferences and scholars draft lengthy manuals and handbooks that purport to explain the current state of the LOAC and international law generally. While laudable to some extent, it is important to understand the motivations and interests of the experts who conduct these projects. For example, humanitarian groups are often driven by their interest in protecting victims of armed conflict and state violence and are not motivated by the desire to protect states' military and operational interests. Similarly, academics are driven by theoretical and conceptual clarity in the law, whereas conceptual and theoretical incongruence or unclarity may reflect states' interests in operational flexibility, or unwillingness or inability to agree with other states on applicable norms. Likewise, the core function of international tribunals is dispute adjudication, not law creation or refinement.

The point is not to diminish or criticize these efforts. Rather, it is to stress the importance of state engagement in this area. At the very least, states must be willing to publicly assert when they disagree with statements of law from these various nonstate efforts.

Based on recent trends, any state development of the LOAC in the near future will be through customary international law (CIL). Of course, as noted above, CIL development is difficult and raises several problematic questions. For example, how does the international community reconcile inconsistencies in the practice of states? Is it possible to deduce specific rules from general principles? When is a state providing clarity on a view versus making a statement of opinio juris? These, along with other underlying issues, must be addressed. As Michael Schmitt and Sean Watts note, "[S]tates' legal agencies and agents should be equipped, organized, and re-empowered to participate actively in the interpretation and development of IHL."

However, the possibility that states will develop new LOAC treaties should not be completely dismissed. The devastating effects of weaponizing new technologies may eventually incentivize states to engage in the development of conventional law. For example, a significant vulnerability for an advanced state engaged in an armed conflict is its reliance on the cyber domain to operate the critical infrastructure essential for societal functions. The catastrophic results of losing the services provided by critical infrastructure are immense and potentially could result in a state's no longer being capable of conducting military operations. Therefore, recognizing the potential adverse consequences of such a cyberattack, advanced states may choose to come together to develop a narrow treaty that provides heightened protections for critical infrastructure during an armed conflict.

As Geoffrey Corn has discussed with the author, adopting narrowly scoped international agreements to avoid potentially catastrophic consequences of armed conflict is not without precedent. For example, the 1976 Environmental Modification Treaty (ENMOD) prohibits the use of environmental modification techniques having widespread, long-lasting or severe effects as the means of destruction, damage or injury to any other state party. The ENMOD Convention was negotiated during a period of heightened international concern about the protection of the environment during armed conflict. By the 1970s, the international community became increasingly aware that the toll of modern armed conflicts went far beyond human suffering and damage to physical property but also led to extensive destruction and degradation to the natural environment. Most notably, the widespread use of the defoliant Agent Orange in Vietnam resulted in environmental contamination leading to significant international criticism and concern. This widespread concern, coupled with the recognition that weaponizing environmental modification techniques could have devastating global effects, brought states together to develop the ENMOD Convention. In similar fashion, states may find it necessary today to develop specific treaty protections in response to global threats posed by new technologies.

This is not to say that the LOAC necessarily will progress through the development of unique rules for narrowly tailored subareas. Indeed, many states are asserting that the LOAC as a whole is up to the task of regulating all forms of armed conflict regardless of operational domain. These states seek to ensure the LOAC's development through the interaction of the structural principles of military necessity and humanitarian considerations; its cardinal principles of distinction, proportionality, and the prevention of unnecessary suffering; and its general rules governing the conduct of hostilities. States may determine that it does not serve their interests to develop the law in a compartmentalized fashion but, rather, holistically as a general body of law.

How the law develops is open to debate, but what is starkly apparent is that states must reassert their traditional stewardship over the LOAC and proactively address new legal questions. Otherwise, the LOAC will become increasingly detached from contemporary warfare as nonstate institutions fill the void without necessarily addressing state interests. This is, of course, dangerous, as it is the LOAC that ensures military necessity and humanity remain in balance and warfare does not devolve into the brutality and savagery that has for so long defined conflict.

Topics: International Law: LOAC

Tags: Geneva Convention, international law: LOAC

Shane R. Reeves is a Colonel in the United States Army. He is an Associate Professor and the Deputy Head of the Department of Law at the United States Military Academy, West Point, New York (shane.reeves@usma.edu). The views expressed here are his personal views and do not necessarily reflect those of the Department of Defense, the United States Army, the United States Military Academy, or any other department or agency of the United States Government. The analysis presented here stems from his academic research of publicly available sources, not from protected operational information.

LAWFARE

IRAN

Was the Soleimani Killing an Assassination?

By **Shane Reeves**, **Winston Williams** Friday, January 17, 2020, 2:12 PM

The Jan. 3 killing of Major General Qassem Soleimani, the head of Iran's Quds Force, has generated a robust conversation in the media on whether the air strike should be characterized as an "assassination." Explaining its decision not to use the term in referring to the killing, the Associated Press wrote that doing so "would require that the news service decide that the act was a murder, and because the term is politically freighted." NPR's public editor, meanwhile, said that the radio service "feel[s] it is an appropriate use of the word, which is defined as the killing of a political leader by surprise." This debate over whether the action was an assassination is unhelpful in determining whether there was a legal basis under international law for the air strike. While the United States prohibits assassination as a matter of national policy through Executive Order (EO) 12333, not every killing violates this ban. Furthermore, even if the killing did not have an international legal basis, it may not necessarily constitute an assassination under the U.S. government's definition of the term.

EO 12333 grew out of President Ford's 1976 EO 11905, which "prohibited any member of the U.S. government from engaging or conspiring to engage in any political assassination." This executive order was promulgated to address concerns that emerged from the Church Committee, a Senate committee charged with investigating potential illegal activities by the intelligence community. In the recommendation section of its interim report, the committee condemned the "use of assassination as a tool of foreign policy."

EO 11905 was superseded by President Carter's EO 12036, which, in turn, was followed by President Reagan's 1981 EO 12333. This final order expressly states in paragraph 2.11 that "no person employed by or acting on behalf of the United States Government shall engage in or conspire to engage in assassination." Despite a number of subsequent amendments to the executive order, this paragraph has remained unchanged through the various presidential administrations. However, the term "assassination" was left undefined in the order.

The most helpful government document explaining how the U.S. approaches assassination in regard to a military operation is a 1989 memorandum coordinated with and concurred in by the Department of State's legal adviser, the Central Intelligence Agency's general counsel, the National Security Council's legal adviser, the Department of Justice Office of Legal Policy, and the civilian and military legal advisers in the Department of Defense. The memorandum was drafted by Hays Parks, thenchief of the International Law Branch, International Affairs Division in the Army's Office of the Judge Advocate General. The memorandum was drafted to "explore assassination in the context of national and international law to provide guidance in revision" on the U.S. Army's Field Manual on the Law of Land Warfare to ensure the document was consistent with EO 12333. Accordingly, the Parks memorandum is concerned primarily with the applicability of international law to these situations. While we recommend reading the entire eight-page document, three points are worth highlighting.

First, the Parks memorandum defines an assassination as an act of murder for political purposes. As an example, Parks cites to a 1978 killing of a Bulgarian defector by Bulgarian State Security agents on the streets of London with a poison-tipped umbrella. (For a more recent example along similar lines, consider the Feb. 13, 2017, killing of Kim Jong-nam, the half-brother of Kim Jong-un, with the nerve agent VX in Kuala Lumpur's international airport terminal.) The Parks memorandum definition was further accepted in a January 2002 Congressional Research Service (CRS) report, which stated that "an assassination may be viewed as an intentional killing of a targeted individual committed for political purposes."

Second, the memo and the CRS report both recognize that the term "assassination" may have different connotations depending on whether the act takes place in wartime or peacetime. While a "political" murder is illegal in either situation, in armed conflict there is greater allowance for violence. In such circumstances, the use of violence based on an individual's status or conduct could be lawful as a matter of first resort. Therefore, if an individual is a combatant, a member of an organized armed group, or a direct participant in hostilities, targeting that individual is obviously not an assassination.

Conversely, absent an armed conflict, there is a different set of rules and lethal force is expected to be used only as a last resort, the memorandum states. Article 2(4) of the U.N. Charter requires states to "refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations." This prohibition has two exceptions—the most relevant being Article 51's recognition of a state's inherent right of self-defense. Also, according to the Parks memorandum, if the right of self-defense is triggered, then there is international legal justification for counteracting an ongoing or imminent threat.

Third, the Parks memorandum concludes that an "overt use of military force against legitimate targets in time of war, or against similar targets in time of peace where such individuals or groups pose an immediate threat to the United States citizens or the national security of the United States, as determined by competent authority, does not constitute assassination" and therefore "would not be prohibited by the proscription in EO 12333 or by international law."

What EO 12333 and the Parks memorandum suggest is that there is no point to continuing to debate whether the drone strike on Soleimani was an assassination without first determining the legality under international law of the United States's action. Only after determining whether the strike was unlawful in the context of an armed conflict or was not a legitimate act of self-defense does the possibility of assassination arise.

Under international law, if the strike took place during an international armed conflict and Soleimani was targeted in his role as the head of the Quds Force, then it was lawful. If the strike occurred during a non-international armed conflict, and he was the operational leader of the militia group (or perhaps a military adviser to that group), then it would also be lawful. If the strike was done outside of armed conflict, and the United States properly acted in self-defense to prevent imminent attacks organized and/or controlled by Soleimani, then again it would be lawful.

If none of the above circumstances occurred, the United States did not have a legal basis for the air strike and committed an unlawful act under international law. But this would not necessarily make the air strike an assassination as prohibited by EO 12333. Under the Parks memorandum and CRS report, to be defined as such, the killing must have a political purpose. Whether there is a political purpose or not for the Soleimani air strike may be a relevant follow-on question. However, it is a subjective analysis that has no bearing on the lawfulness of the air strike under international law—and, consequently, has limited initial legal value.

For this reason, arguing whether the Soleimani air strike was an assassination is premature without first addressing the underlying question: Was the strike legal or not?

Topics: Iran

Tags: Iran, International Law, Law of Armed Conflict, Qassem Soleimani

---

Shane R. Reeves is a Colonel in the United States Army. He is an Associate Professor and the Deputy Head of the Department of Law at the United States Military Academy, West Point, New York (shane.reeves@usma.edu). The views expressed here are his personal views and do not necessarily reflect those of the Department of Defense, the United States Army, the United States Military Academy, or any other department or agency of the United States Government. The analysis presented here stems from his academic research of publicly available sources, not from protected operational information.

Winston Williams is a lieutenant colonel in the United States Army. He is an associate professor in the Department of Law at the United States Military Academy, West Point, New York. The views expressed here are his personal views and do not necessarily reflect those of the Department of Defense, the United States Army, the United States Military Academy, or any other department or agency of the United States Government. The analysis presented here stems from academic research of publicly available sources, not from protected operational information.

Protecting Critical Infrastructure in Cyber Warfare: Is It Time for States to Reassert Themselves?

David A. Wallace[†*] *and Shane R. Reeves*[**]

When Russia uses a "combination of instruments, some military and some non-military, choreographed to surprise, confuse, and wear down" Ukraine, it is termed hybrid warfare.[1] *The term also refers to conflicts, which are both international and non-international in character, such as the ongoing conflict in Syria.*[2] *Overlapping conventional and asymmetric tactics in an armed conflict — as when Russia simultaneously conducted cyber-attacks during a conventional invasion of Georgia in 2008 — also gets the hybrid warfare label.*[3] *Or, as Professor Bobby Chesney wrote regarding U.S. operations in Somalia, hybrid warfare can include "a sophisticated approach that layers together a panoply of low-visibility (to*

* Professor & Head, Department of Law, United States Military Academy, West Point.

** Associate Professor & Deputy Head, Department of Law, United States Military Academy, West Point.

1 *See What Russia Wants: From Cold War to Hot War*, ECONOMIST (Feb. 12, 2015), https://www.economist.com/briefing/2015/02/12/from-cold-war-to-hot-war [https://perma.cc/Y89X-49U3].

2 *See generally* David Wallace, Amy McCarthy & Shane R. Reeves, *Trying to Make Sense of the Senseless: Classifying the Syrian War Under the Law of Armed Conflict*, 25 MICH. ST. INT'L L. REV. 555 (2017) (discussing the various elements of conflict in Syria, to include state and non-state factions).

3 *See* Shane R. Reeves & Robert E. Barnsby, *The New Griffin of War: Hybrid International Armed Conflicts*, HARV. INT'L REV., Winter 2013, at 16-17 (discussing the international legal challenges presented by hybrid warfare).

the public both here and there) tools" to conduct counter-terrorism operations in failing states.[4]

In other words, "hybrid warfare" has become a shorthand way to describe the various complexities of the modern battlefield. Hybrid warfare — regardless how the term is used — clearly raises several challenging and important legal issues. Some of these issues include finding a workable approach to enforcing the principle of distinction, properly classifying conflicts, and understanding the roles of the military and law enforcement in contemporary warfare. Yet, perhaps no aspect of hybrid warfare generates more legal questions than operations in cyberspace.

Cyberspace, defined as "a global domain within the information environment that encompasses the interdependent networks of information technology infrastructures, including the internet and telecommunication networks,"[5] *is quickly becoming the decisive battleground in warfare.*[6] *National armed forces, and more specifically technologically advanced militaries, rely upon their information networks for command and control, intelligence, logistics, and weapon technology, making protecting these assets a priority.*[7] *Arguably, however, the greatest vulnerability for an advanced State engaged in an armed conflict is its reliance on the cyber domain to operate the critical infrastructure essential for societal functions.*

The catastrophic results of losing the essential services provided by critical infrastructure are immense and, potentially, could result in a State being incapable of conducting military operations. Recognizing this vulnerability, this Essay therefore critically examines how the law of armed conflict protects such objects and activities. In doing so, the Essay concludes that heightened protections for critical infrastructure from cyber-attacks are necessary and suggests looking to the existing framework of special precautionary protections as a model for greater legal safeguards.

---

[4] Robert Chesney, *American Hybrid Warfare: Somalia as a Case Study in the Real American Way of War in 2016*, LAWFARE (Oct. 17, 2016, 7:06 AM), https://www.lawfareblog.com/american-hybrid-warfare-somalia-case-study-real-american-way-war-2016 [https://perma.cc/YNZ6-496H].

[5] U.S. DEP'T OF DEF., QUADRENNIAL DEFENSE REVIEW REPORT 37 (2010) [hereinafter QUADRENNIAL REPORT].

[6] *See, e.g.*, RICHARD A. CLARKE & ROBERT K. KNAKE, CYBER WAR 69 (2010); Stephen W. Korns & Joshua E. Kastenberg, *Georgia's Cyber Left Hook*, PARAMETERS, Winter 2008-2009, at 60 (discussing the desperate actions of the Georgian government after it found itself unable to communicate through the internet during the 2008 Georgian-Russian conflict).

[7] *See* QUADRENNIAL REPORT, *supra* note 5, at 37.

TABLE OF CONTENTS

> "The single biggest existential threat that's out there, I think, is cyber."[8]
>
> —Admiral (ret.) Michael Mullen

INTRODUCTION

As the Chairman of the Joint Chiefs of Staff, Admiral Michael Mullen served as the principal military adviser to Presidents George W. Bush and Barack Obama, and was the senior ranking member of the Armed Forces of the United States.[9] As such, his views on existential threats

[8] Micah Zenko, *The Existential Angst of America's Top Generals*, FOREIGN POL'Y (Aug. 4, 2015, 9:00 AM), https://foreignpolicy.com/2015/08/04/the-existential-angst-of-americas-top-generals-threat-inflation-islamic-state [https://perma.cc/3WC4-B85K].

[9] *See Chairman of the Joint Chiefs of Staff*, JOINT CHIEFS OF STAFF, http://www.jcs.mil/About/The-Joint-Staff/Chairman (last visited Dec. 26, 2019) [https://perma.cc/JR7R-9YD6]. Admiral Mullen became the seventeenth Chairman of the Joint Chiefs of Staff on October 1, 2007. *17th Chairman of the Joint Chiefs of Staff: Admiral Michael Glenn Muller*, JOINT CHIEFS OF STAFF, https://www.jcs.mil/About/The-Joint-Staff/Chairman/Admiral-Michael-Glenn-Mullen/ (last visited Dec. 26, 2019) [https://perma.cc/SUQ7-SE2J].

facing the country are not only relevant and weighty, but also alarming. It is not difficult to understand Admiral Mullen's fears as cyberspace increasingly allows an adversary to exploit, disrupt, deny, and degrade almost all of a State's important military and civilian computer networks and related systems.[10] Most concerning, these cyber vulnerabilities include those that run a State's critical infrastructure — whether it be the electronic grid, commercial or market activities, transportation networks, water and distribution systems, or emergency services. Incapacitating or destroying any of these systems or assets would "have a debilitating impact on security, national economic security, national public health or safety"[11] and adversely affect thousands (perhaps millions) of civilians. Consequently, social unrest and chaos would follow.[12]

The threat of a paralyzing cyber-attack on critical infrastructure is neither theoretical nor academic. It is real. President Obama made this clear in 2013 when he stated:

> Repeated cyber intrusions into critical infrastructure demonstrate the need for improved cybersecurity. The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront. The national and economic security of the United

[10] *See* U.S. DEP'T OF DEF., DEPARTMENT OF DEFENSE STRATEGY FOR OPERATING IN CYBERSPACE 3-4 (2011).

[11] Exec. Order No. 13,636, 78 Fed. Reg. 11,739, 11,739 (Feb. 12, 2013).

[12] *See* Bret Brasso, *Cyber Attacks Against Critical Infrastructure Are No Longer Just Theories*, FIREEYE (Apr. 29, 2016), https://www.fireeye.com/blog/executive-perspective/2016/04/cyber_attacks_agains.html [https://perma.cc/54HM-CHEN]. Recognizing the consequences associated with cyber-attacks on critical infrastructure, the United Nations Group of Governmental Experts ("UNGGE") on Information Security specifically noted in their 2015 report that "[a] State should not conduct or knowingly support [information and communications technology] activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public." U.N. Grp. of Governmental Experts, *Developments in the Field of Information and Telecommunications in the Context of International Security*, ¶ 13(f), U.N. Doc. A/70/174 (July 24, 2015), http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174 [https://perma.cc/U5A8-JEWR]. The 2015 UNGGE report contains recommendations developed by governmental experts from twenty States addressing threats from uses of information and communications technologies by States and non-State actors alike and, in doing so, builds upon reports issued in 2010 and 2013. *Id.* at 4. These reports have become a significant focal point for international discussions on the applicability of international law to States with respect to cyberspace and operations. Elaine Korzak, *The 2015 GGE Report: What Next for Norms in Cyberspace?*, LAWFARE (Sept. 23, 2015, 8:32 AM), https://www.lawfareblog.com/2015-gge-report-what-next-norms-cyberspace [https://perma.cc/9RNH-QS2L].

> States depends on the reliable functioning of the Nation's critical infrastructure in the face of such threats.[13]

More recently, in describing his concerns about a cyber-attack against critical infrastructure, former National Security Agency Director Admiral Michael Rogers predicted, "[i]t is only a matter of the when, not the if, that we are going to see something traumatic."[14] Unfortunately, State activities in cyberspace have proven these statements true. For example, on December 23, 2015, a cyber-attack shut down Ukraine's relatively secure power grid.[15] More specifically, the Ukrainian Kyivoblenergo, a regional electricity distribution company, suffered severe power outages affecting 225,000 customers due to a malicious malware.[16] Not long after the incident occurred, the Ukrainian government publicly attributed the highly sophisticated cyber intrusion[17] to Russian security services.[18]

While similar events are transpiring regularly,[19] the attack on the Ukrainian critical infrastructure is particularly important as it took place during a period of armed conflict.[20] Undoubtedly, it is relevant

---

[13] Exec. Order No. 13,636, 78 Fed. Reg. at 11,739.

[14] Amelia Smith, *China Could Shut Down U.S. Power Grid with Cyber Attack, Says NSA Chief*, NEWSWEEK (Nov. 21, 2014, 11:07 AM), http://www.newsweek.com/china-could-shut-down-us-power-grid-cyber-attack-says-nsa-chief-286119 [https://perma.cc/Y3XR-N4LV].

[15] *See* Kim Zetter, *Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid*, WIRED (Mar. 3, 2016, 7:00 AM), https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid [https://perma.cc/54ZC-J35V].

[16] *See* ROBERT M. LEE ET AL., ELEC. INFO. SHARING & ANALYSIS CTR., ANALYSIS OF THE CYBER ATTACK ON THE UKRAINIAN POWER GRID, at iv (2016), https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf [https://perma.cc/Z3FR-LAZU].

[17] *See* Zetter, *supra* note 15.

[18] *See* LEE ET AL., *supra* note 16, at iv.

[19] For example, Russia recently used malicious computer code known as Triton to gain control over a safety shut-off system — considered critical to defending against catastrophic events — at a petrochemical plant in Saudi Arabia. *See* Dustin Volz, *Researchers Link Cyberattack on Saudi Petrochemical Plant to Russia*, WALL ST. J. (Oct. 23, 2018, 3:20 PM), https://www.wsj.com/articles/u-s-researchers-link-cyberattack-on-saudi-petrochemical-plant-to-russia-1540322439 [https://perma.cc/56SV-VQB9]. This intrusion is the first reported breach of a safety system at an industrial plant. *See id.*

[20] Although the precise contours of the armed conflict in the Ukraine are difficult to determine, it appears to be international and non-international armed conflicts occurring in parallel. *See* Shane R. Reeves & David Wallace, *The Combatant Status of the "Little Green Men" and Other Participants in the Ukraine Conflict*, 91 INT'L L. STUD. 361, 372-83 (2015); *see also International Armed Conflict in Ukraine*, RULAC, http://www.rulac.org/browse/conflicts/international-armed-conflict-in-ukraine [https://perma.cc/E3UU-2HMB] (last updated Sept. 12, 2017). As an international armed conflict was occurring at the time of the cyber-attack on the power grid, the law of armed conflict applied. *See id.*

and important to understand how international law regulates interactions between States when one intrudes upon the other's critical infrastructure outside of armed conflict.[21] However, this Essay focuses on the equally important topic of cyber targeting of critical infrastructure during a period of armed conflict — such as the Russian hack of the Ukrainian power grid — and whether the current normative framework of the law of armed conflict provides sufficient protections from such attacks.[22]

Through this analysis, it becomes apparent that existing protections for critical infrastructure in armed conflict are inadequate and heightened legal safeguards are necessary. To support this proposition, the Essay begins with a brief description of critical infrastructure and explains why these systems are vulnerable in cyberspace. A general overview of the law of armed conflict's provisions on targeting follows. The Essay then applies these principles and rules to critical infrastructure in cyberspace to illustrate that the existing law — *lex lata*[23] — does not go far enough in protecting these essential assets. The Essay thus concludes with a *lex ferenda* argument[24] in favor of a new treaty that provides additional protections against cyber-attacks for critical infrastructure during armed conflict.

I. WHAT IS CRITICAL INFRASTRUCTURE? WHY SHOULD WE WORRY?

There is no universal definition of "critical infrastructure." Instead, States subjectively determine the assets, systems, or capabilities that are critical to their national security. In the United States, for example,

[21] For a comprehensive general overview of international law in cyberspace, see generally INT'L GRP. OF EXPERTS, TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS (Michael N. Schmitt et al. eds., 2017) [hereinafter TALLINN MANUAL 2.0].

[22] The law of armed conflict, which is often also called international humanitarian law, is a "set of rules which seek, for humanitarian reasons, *to limit the effects of armed conflict*. It protects persons who are not or are no longer participating in the hostilities and restricts the means and methods of warfare." ADVISORY SERV. ON INT'L HUMANITARIAN LAW, INT'L COMM. OF THE RED CROSS, WHAT IS INTERNATIONAL HUMANITARIAN LAW? (2004), https://www.icrc.org/en/doc/assets/files/other/what_is_ihl.pdf; *see also* U.S. DEP'T OF DEF., DIRECTIVE 2311.01E, ¶ 3.1 (2006), https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/231101e.pdf [https://perma.cc/8S47-QPA8] (defining the law of war as the part of international law that regulates the "conduct of armed hostilities" and is often called "the law of armed conflict").

[23] *Lex lata* is defined as "what the law is." J. Jeremy Marsh, Lex Lata *or* Lex Ferenda*? Rule 45 of the ICRC Study on Customary International Humanitarian Law*, 198 MIL. L. REV. 116, 117 (2008).

[24] *Lex ferenda* is defined as "what the law should be." *Id.*

critical infrastructure is defined as those "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[25] Characterized in a slightly different manner, critical infrastructure are assets or systems vital for the maintenance of essential societal functions[26] and serve as the backbone of a State's economy, security, and health.[27]

Importantly, most of the assets or services essential to a society are interconnected. Damage, destruction, or disruption in one system, therefore, would naturally have significant negative consequences in other important systems necessary for the operation of an advanced State.[28] Recognizing this interconnectedness risk, States increasingly characterize large groupings of assets, systems, or capabilities as "critical infrastructure." By doing so, States are attempting to protect not just a particular asset or service, but rather the entire ecosystem that underlies its national security.[29] For example, the United States Department of Homeland Security — aside from the generic definition provided above — now identifies sixteen critical infrastructure sectors including: chemical, commercial facilities, communications, critical manufacturing, dams, defense industrial base, emergency services,

[25] Critical Infrastructures Protection Act of 2001, 42 U.S.C. § 5195c (2019). The statute provides, among other things, "that any physical or virtual disruption of the operation of the critical infrastructures of the United States be rare, brief, geographically limited in effect, manageable, and minimally detrimental to the economy, human and government services, and national security of the United States . . . ." *Id.*

[26] *Migration and Home Affairs: Critical Infrastructure*, EUR. COMM'N, https://ec.europa.eu/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure_en (last visited Dec. 26, 2019) [https://perma.cc/LF9P-DUEZ].

[27] *See CISA Infrastructure Security: Supporting Policy and Doctrine*, U.S. DEP'T OF HOMELAND SEC., https://www.dhs.gov/what-critical-infrastructure (last visited Dec. 26, 2019) [https://perma.cc/K9SQ-8QYU].

[28] *See generally Critical Infrastructure Sectors*, U.S. DEP'T OF HOMELAND SEC., https://www.dhs.gov/critical-infrastructure-sectors (last visited Nov. 21, 2018) [https://perma.cc/V55P-KP4T] [hereinafter *Critical Infrastructure Sectors*] (listing sixteen United States critical infrastructure sectors).

[29] In other words, a State is communicating to potential adversaries the importance of these particular assets and, consequently, the severe ramifications if attacked. While what exactly those ramifications may be is outside the scope of this Essay, it is important to note, "[t]he use of force threshold, wherever it may presently lie, will almost certainly drop in lock step with the increasing dependency of states on cyberspace." Michael N. Schmitt, The Law of Cyber Warfare: Quo Vadis?, 25 STAN. L. & POL'Y REV. 269, 281 (2014) [hereinafter *Law of Cyber Warfare*] ("In particular, operations that non-destructively target critical infrastructure may come to be viewed by states as presumptive uses of force.").

energy, financial services, food and agriculture, government facilities, healthcare and public health, information technology, nuclear, transportation systems, and water and wastewater systems.[30]

The failure of critical infrastructure, regardless of the reason, is potentially catastrophic. Although an August 2003 blackout was neither cyber-related nor did it occur during an armed conflict, the event's widespread disruption of power over parts of eight U.S. states illustrates the point.[31] On one afternoon in the middle of August, a power line in northern Ohio, softened by the heat of summer, brushed against some trees and triggered an automatic shutdown of the power line. Over the next few hours, as technicians tried to understand the nature and scope of the problem, three other power lines sagged into trees causing additional shutdowns.[32] Eventually, the entire electrical system was overtaxed.[33] Approximately 50 million people lost power, eleven individuals died, and economic damages escalated into the billions.[34] Additionally, the power outage stranded thousands of commuters, disrupted air traffic across the United States, flooded hospitals with patients complaining of heat injuries, and required mandatory evacuations of buildings, tunnels, and other public areas.[35]

As the 2003 blackout shows, critical infrastructure is interconnected and interdependent — an outwardly insignificant incident in northern Ohio triggered not only the massive loss of electrical power in one town, but severely disrupted power systems throughout the United States. Yet, vulnerabilities in systems as important as the electric "grid" continue to exist and are numerous and obvious. The entire system consists of miles of high-voltage and low-voltage power lines, distribution transformers,

---

[30] *See* U.S. DEP'T OF HOMELAND SEC., *Critical Infrastructure Sectors*, *supra* note 28.

[31] *See* James Barron, *The Blackout of 2003: The Overview; Power Surge Blacks Out Northeast, Hitting Cities in 8 States and Canada; Midday Shutdowns Disrupt Millions*, N.Y. TIMES (Aug. 15, 2003), https://www.nytimes.com/2003/08/15/nyregion/blackout-2003-overview-power-surge-blacks-northeast-hitting-cities-8-states.html [https://perma.cc/ZHX4-KJNC]. The blackout affected the U.S. states of Ohio, Michigan, Pennsylvania, New York, Vermont, Massachusetts, Connecticut, and New Jersey, and the Canadian province of Ontario. *See id.*

[32] *See* JR Minkel, *The 2003 Northeast Blackout — Five Years Later*, SCI. AM. (Aug. 13, 2008), https://www.scientificamerican.com/article/2003-blackout-five-years-later [https://perma.cc/M72K-SSTN].

[33] *See id.* An April 2004 report on the incident found that systemic problems with the grid, and the cascading nature of the event, caused the blackout. *See generally* U.S.-CAN. POWER SYS. OUTAGE TASK FORCE, FINAL REPORT ON THE AUGUST 14, 2003 BLACKOUT IN THE UNITED STATES AND CANADA: CAUSES AND RECOMMENDATIONS (2004).

[34] *See* Minkel, *supra* note 32. Estimates of the damage from the blackout were estimated at $6 billion. *See id.*

[35] *See* Barron, *supra* note 31.

and connections between thousands of power plants to hundreds of millions of electricity customers.[36] What becomes apparent is that any damage, disruption, or even delay along the electricity grid continuum is potentially devastating and could have a cascading negative effect on the economic and security well-being of an affected State.

The United States became acutely aware of such risks to critical infrastructure following the terrorist attacks of September 11, 2001. In February 2003, the United States government released *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* in an effort to reduce America's vulnerabilities to acts of terrorism.[37] The report observed that the facilities, systems, and functions that comprise an advanced society's critical infrastructure are highly sophisticated and complex.[38] Additionally, the report found that "our most critical infrastructures typically interconnect and, therefore, depend on the continued availability and operation of other dynamic systems and functions."[39] E-commerce, for example, depends on electricity (as well as information and technology), and protecting and maintaining these ancillary systems is a necessity for internet trade.[40] The report thus concludes: "[g]iven the dynamic nature of these interdependent infrastructures and the extent to which our daily lives rely on them, a successful terrorist attack to disrupt or destroy them could have tremendous impact beyond the immediate target and continue to reverberate long after the immediate damage is done."[41]

The report's logic applies equally to a cyber-attack against critical infrastructure, and its warning about the potential for such an incident is ever more prescient. For example, in 2013, an Iranian hacker named Hamid Firoozi — most likely working on behalf of the Iranian government[42] — gained remote access to the Bowman Avenue Dam in

---

[36] *See Electricity Explained: How Electricity Is Delivered to Consumers*, U.S. ENERGY INFO. ADMIN., https://www.eia.gov/Energyexplained/index.cfm?page=electricity_delivery (last updated Oct. 11, 2019) [https://perma.cc/T6JS-K9KE].

[37] *See* U.S. DEP'T OF HOMELAND SEC., THE NATIONAL STRATEGY FOR THE PHYSICAL PROTECTION OF CRITICAL INFRASTRUCTURES AND KEY ASSETS (2003), https://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf [https://perma.cc/G62A-MY6W].

[38] *See id.* at 6.

[39] *Id.*

[40] *See id.* (noting that, similarly, transportation and distribution systems are necessary to assure the delivery of fuel to generate power).

[41] *Id.* at 7.

[42] *See* Sealed Indictment at 1-2, United States of America v. Ahmad Fathi et al., No. 16CR00048, 2016 WL 1291521 (S.D.N.Y. Jan. 21, 2016) [hereinafter Sealed Indictment].

Rye Brook, New York (fifteen miles north of New York City).[43] Access to the dam gave Firoozi the ability to remotely operate and manipulate the sluice gate, which is responsible for controlling water levels and flow rates.[44] Fortunately, the dam operators had manually disconnected the sluice gate for maintenance prior to the hack.[45] While Firoozi seemingly failed, he may have in fact been extremely successful, as he was likely conducting "a dry run for a more disruptive invasion of, say, a major hydroelectric generator or some other grand and indispensable element of the nation's power grid."[46]

The strategic importance of critical infrastructure coupled with the numerous vulnerabilities found within these assets and systems make cyber-attacks increasingly attractive to potential adversaries of any advanced State. This is especially true during a period of armed conflict. The United States, in its Department of Defense 2015 Cyber Strategy, recognizes this fact by noting "[d]uring a conflict, the Defense Department assumes that a potential adversary will seek to target U.S. or allied critical infrastructure and military networks to gain a strategic advantage."[47] The report goes on to assume that all critical

[43] *See* Tom Ball, *Top 5 Critical Infrastructure Cyber Attacks*, COMPUTER BUS. REV. (July 18, 2017), https://www.cbronline.com/cybersecurity/top-5-infrastructure-hacks [https://perma.cc/HT9N-ZMAQ].

[44] *See* Sealed Indictment, *supra* note 42, at 14-15.

[45] *See id.* at 15.

[46] Joseph Berger, *A Dam, Small and Unsung, Is Caught Up in an Iranian Hacking Case*, N.Y. TIMES (Mar. 25, 2016), https://www.nytimes.com/2016/03/26/nyregion/rye-brook-dam-caught-in-computer-hacking-case.html [https://perma.cc/9EAC-AXGD]. Since the incident at the Bowman Avenue Dam, cyber intrusions attempting to affect the American water supply have continued with increasing effectiveness. *See, e.g.*, Ari Mahairas & Peter J. Beshar, Opinion, *A Perfect Target for Cybercriminals*, N.Y. TIMES (Nov. 19, 2018), https://www.nytimes.com/2018/11/19/opinion/water-security-vulnerability-hacking.html [https://perma.cc/L7WW-8GZ2] (discussing recent examples of cyber-attacks on water and sewer utilities). The authors assert, "[t]he concept of damaging a society by attacking its water supply is as old as warfare itself. . . . These days, the threat is more pernicious than ever: Destruction and disruption that once required explosives can be achieved with keystrokes." *Id.*

[47] U.S. DEP'T OF DEF., THE DEPARTMENT OF DEFENSE CYBER STRATEGY 2 (2015), https://archive.defense.gov/home/features/2015/0415_cyber-strategy/final_2015_dod_cyber_strategy_for_web.pdf [hereinafter DOD CYBER STRATEGY]. The Department of Defense released an updated version of the Cyber Strategy document in September of 2018. *See* Mark Pomerleau, *DoD Releases First New Cyber Strategy in Three Years*, FIFTH DOMAIN (Sept. 18, 2018), https://www.fifthdomain.com/dod/2018/09/19/department-of-defense-unveils-new-cyber-strategy [https://perma.cc/4QUV-6ED7]. While the updated strategy supersedes the 2015 document, it re-emphasizes the importance of protecting critical infrastructure. *See* U.S. DEP'T OF DEF., SUMMARY: DEPARTMENT OF DEFENSE CYBER STRATEGY 2 (2018), https://media.defense.gov/2018/sep/18/2002041658/-1/-1/1/cyber_strategy_summary_final.pdf [https://perma.cc/NZZ5-UL8C]

infrastructure is targetable and gives examples of an adversary attacking "an industrial control system (ICS) on a public utility to affect public safety" or entering "a network to manipulate health records to affect an individual's well-being."[48] The Cyber Strategy concludes that the purpose of any such attack is to undercut the United States' economic and national security — despite the inevitable death and destruction that will ensue — and therefore protecting critical infrastructure is of paramount interest.[49] The following Part discusses how the law currently protects such assets during a period of armed conflict.

II. AN OVERVIEW OF TARGETING UNDER THE LAW OF ARMED CONFLICT

The law of armed conflict regulates the targeting of both persons and objects, regardless of the means or methods used by the parties, in both international and non-international armed conflicts.[50] However, of importance to understanding the extant legal protections for critical infrastructure in armed conflict is the law of targeting[51] as it specifically relates to objects. While there are several law of armed conflict principles and rules applicable to the targeting of objects,[52] underlying each of these individual norms is a compromise between two diametrically opposed impulses: military necessity and humanitarian considerations.[53] Therefore, before delving into the specifics of the law

("[T]he Department seeks to preempt, defeat, or deter malicious cyber activity targeting U.S. critical infrastructure that could cause a significant cyber incident . . . .").

48 DOD CYBER STRATEGY, *supra* note 47, at 2.

49 *See id.*

50 TALLINN MANUAL 2.0, *supra* note 21, at 414.

51 The term "targeting" is broadly understood as using violence against people or objects in the context of an armed conflict. *See* Gary P. Corn et al., *Targeting and the Law of Armed Conflict*, *in* U.S. MILITARY OPERATIONS: LAW, POLICY, AND PRACTICE 167, 172, 173 (Geoffrey S. Corn et al. eds., 2016). The law of targeting is therefore that subset of the law of armed conflict that regulates how that violence is conducted. *See id.* at 172-73 ("[I]t is universally recognized that during *any* armed conflict, the warring parties' discretion to employ violence is not legally unfettered."); *see also* YORAM DINSTEIN, THE CONDUCT OF HOSTILITIES UNDER THE LAW OF INTERNATIONAL ARMED CONFLICT 126 (1st ed. 2004) (stating that targeting is "the selection of appropriate targets from a list of military objectives — as well as the choice of weapons and ordnance").

52 *See* WILLIAM H. BOOTHBY, THE LAW OF TARGETING 60-64 (2012) [hereinafter LAW OF TARGETING].

53 *See* Kjetil Mujezinovi Larsen et al., *Introduction by the Editors: Is There a 'Principle of Humanity' in International Humanitarian Law?*, *in* SEARCHING FOR A 'PRINCIPLE OF HUMANITY' IN INTERNATIONAL HUMANITARIAN LAW 1, 9 (Kjetil Mujezinovi Larsen et al. eds., 2013).

of targeting, a brief discussion on the military necessity-humanity balance is necessary.[54]

A. The Foundation for the Law of Targeting: Military Necessity Versus Humanity

Military necessity[55] is best understood as a broad "attempt to realize the purpose of armed conflict, gaining military advantage," whereas humanitarian considerations are intent on "minimizing human suffering and physical destruction" in warfare.[56] These two broad, often times called "meta," principles[57] are weighed against each other throughout the entirety of the law of armed conflict with every rule or norm — whether treaty- or custom-based — considering both military necessity and the dictates of humanitarian aims.[58] In other words, "it

[54] *See id.*

[55] Francis Lieber stated, "[m]ilitary necessity, as understood by modern civilized nations, consists in the necessity of those measures which are indispensable for securing the ends of the war, and which are lawful according to the modern law and usages of war." FRANCIS LIEBER, INSTRUCTIONS FOR THE GOVERNMENT OF ARMIES OF THE UNITED STATES IN THE FIELD: GENERAL ORDERS NO. 100, at art. 14 (1863), *reprinted in* THE LAWS OF ARMED CONFLICTS 3, 6 (Dietrich Schindler & Ji í Toman eds., 3d ed. 1988) [hereinafter LIEBER CODE]. This definition of military necessity has remained mostly intact in current U.S. doctrine. *See, e.g.*, U.S. DEP'T OF THE ARMY, FIELD MANUAL NO. 27-10, THE LAW OF LAND WARFARE at ¶ 3.a (1956), https://www.loc.gov/rr/frd/Military_Law/pdf/law_warfare-1956.pdf [https://perma.cc/74KQ-ELS6] (defining military necessity as "those measures not forbidden by international law which are indispensable for securing the complete submission of the enemy as soon as possible"). The definition has also survived in academic writing. *See, e.g.*, WILLIAM H. BOOTHBY, WEAPONS AND THE LAW OF ARMED CONFLICT 72 (2009) (citing LIEBER CODE, *supra* note 55, at art. 14).

[56] GARY D. SOLIS, THE LAW OF ARMED CONFLICT: INTERNATIONAL HUMANITARIAN LAW IN WAR 278 (2d ed. 2016).

[57] *See* Brian J. Bill, *The Rendulic 'Rule': Military Necessity, Commander's Knowledge, and Methods of Warfare*, *in* 12 YEARBOOK OF INTERNATIONAL HUMANITARIAN LAW 119, 131 (2009) ("Military necessity is a meta-principle of the law of war . . . in the sense that it justifies destruction in war. It permeates all subsidiary rules."); *see also* DINSTEIN, *supra* note 51, at 16 (comparing the principles at their extremes).

[58] *See* Christopher Greenwood, *Humanitarian Requirements and Military Necessity*, *in* THE HANDBOOK OF INTERNATIONAL HUMANITARIAN LAW 35, 37-38 (Dieter Fleck ed., 2d ed. 2008) (discussing generally how the principles of military necessity and humanity check and balance each other throughout the law of armed conflict); Shane R. Reeves & Jeffrey S. Thurnher, *Are We Reaching a Tipping Point? How Contemporary Challenges Are Affecting the Military Necessity-Humanity Balance*, HARV. NAT'L SECURITY J. FEATURES ONLINE (2013), http://harvardnsj.org/2013/06/are-we-reaching-a-tipping-point-how-contemporary-challenges-are-affecting-the-military-necessity-humanity-balance [https://perma.cc/CG27-CSJM] (explaining that humanity and military necessity must be simultaneously considered in the law of armed conflict).

can be stated categorically that no part" of the law of armed conflict "overlooks military requirements, just as no part . . . loses sight of humanitarian considerations."[59]

This equilibrium is not new to the law of armed conflict. The 1868 St. Petersburg Declaration, which is considered the first major international agreement prohibiting the use of a particular weapon,[60] outlined the relationship, and inherent tension, between military necessity and humanity in renouncing the use of explosive projectiles.[61] A similar check and balance which exists in all subsequent law of armed conflict provisions ensures that "force is applied on the battlefield in a manner allowing for the accomplishment of the mission while simultaneously taking appropriate humanitarian considerations into account."[62] Otherwise, "[i]f military necessity were to prevail completely, no limitation of any kind would [be] imposed on the freedom of action of belligerent States. . . . Conversely, if benevolent humanitarianism were the only beacon to guide the path of the armed forces, war would . . . entail[] no bloodshed, no destruction and no human suffering; in short, war would not [be] war."[63]

The law of armed conflict therefore is a series of "prohibitions, restrictions, and obligations designed to balance a State's interest in effectively prosecuting the war (military necessity) with its interest in minimizing harm to those involved in a conflict."[64] With the law of targeting conceptually best thought of as a subset of the law of armed conflict, the underlying objective of both is the same. Accordingly, the

---

[59] DINSTEIN, *supra* note 51, at 17. Professor Dinstein notes that the law of armed conflict is "predicated on a subtle equilibrium between two diametrically opposed impulses: military necessity and humanitarian considerations." *Id.* at 16.

[60] *See* ADAM ROBERTS & RICHARD GUELFF, DOCUMENTS ON THE LAWS OF WAR 53 (3d ed. 2000). This treaty renounced the employment of any projectile of a weight below 400 grams, which was either explosive or charged with fulminating or inflammable substances. *See* Declaration Renouncing the Use, in Time of War, of Explosive Projectiles Under 400 Grammes Weight, Dec. 11, 1868, 138 C.T.S. 297 [hereinafter 1868 St. Petersburg Declaration], https://ihl-databases.icrc.org/ihl/full/declaration1868 [https://perma.cc/PP3T-ZSFH].

[61] *See* 1868 St. Petersburg Declaration, *supra* note 60; *see also* ROBERTS & GUELFF, *supra* note 60, at 53.

[62] Reeves & Thurnher, *supra* note 58, at 1.

[63] DINSTEIN, *supra* note 51, at 16. The balance between military necessity and humanitarian consideration is the very essence of the law of armed conflict. You see this balance not only at the macro-level, but it permeates down to particular rules and provisions. It is what makes the body of law workable considering what is being regulated — i.e., the worst of human conditions. *See id.*

[64] Michael N. Schmitt & Jeffrey S. Thurnher, "*Out of the Loop": Autonomous Weapon Systems and the Law of Armed Conflict*, 4 HARV. NAT'L SEC. J. 231, 232 (2013).

particular provisions or rules, discussed below, that regulate the targeting of objects will always carefully weigh the violence necessary to accomplish a mission with the need to minimize human suffering and physical destruction during warfare.[65]

B. Targeting and the Law: Distinction, Proportionality, and Precautions in the Attack

The military necessity-humanity balance establishes the foundation for the general principles that regulate hostilities and, more specifically, those relevant to the targeting of an object.[66] Undoubtedly, the most important of these principles is distinction — at times characterized as fundamental or "intransgressible."[67] Since the sole legitimate aim of belligerent hostilities is to weaken and defeat an adversary's military forces,[68] protecting both the civilian population and objects during an armed conflict is important.[69] Referenced in early law of armed conflict provisions, such as the Lieber Code[70] and the St. Petersburg

[65] *See* DINSTEIN, *supra* note 51, at 17; *see also* Shane R. Reeves & David Lai, *A Broad Overview of the Law of Armed Conflict in the Age of Terror*, *in* THE FUNDAMENTALS OF COUNTERTERRORISM LAW 139, 147-49 (Lynne Zusman ed., 2014) ("[M]ilitary necessity is 'discounted in the rules' that comprise the Law of Armed Conflict, with the particular provisions of the law either allowing for violence and destruction or forbidding such conduct out of deference to humanitarian considerations."); Michael N. Schmitt, *Military Necessity and Humanity in International Humanitarian Law: Preserving the Delicate Balance*, 50 VA. J. INT'L L. 795, 799 (2010) [hereinafter *Military Necessity*].

[66] *See* Michael N. Schmitt, *Autonomous Weapon Systems and International Humanitarian Law: A Reply to the Critics*, HARV. NAT'L SEC. J. FEATURES ONLINE 9-10 (2013) [hereinafter *Autonomous Weapon Systems*], https://harvardnsj.org/wp-content/uploads/sites/13/2013/02/Schmitt-Autonomous-Weapon-Systems-and-IHL-Final.pdf [https://perma.cc/DK85-537J] (discussing how the rules act as a safeguard).

[67] Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, 257. The opinion also stated that distinction is one of two "cardinal" principles in the law of armed conflict. *See id.*

[68] *See* Nils Melzer, *The Principle of Distinction Between Civilians and Combatants*, *in* THE OXFORD HANDBOOK OF INTERNATIONAL LAW IN ARMED CONFLICT 296, 297 (Andrew Clapham & Paola Gaeta eds., 2014). The 1868 St. Petersburg Declaration makes a similar statement. *See* 1868 St. Petersburg Declaration, *supra* note 60.

[69] *See* COMMENTARY ON THE ADDITIONAL PROTOCOLS OF 8 JUNE 1977 TO THE GENEVA CONVENTIONS OF 12 AUGUST 1949 at ¶ 1863 (Yves Sandoz et al. eds., 1987) [hereinafter COMMENTARY] (footnotes omitted) ("It is the foundation on which the codification of the laws and customs of war rests: the civilian population and civilian objects must be respected and protected . . . . The entire system established in The Hague in 1899 and 1907 and in Geneva from 1864 to 1977 is founded on this rule . . . .").

[70] *See* LIEBER CODE, *supra* note 55, at art. 22 ("Nevertheless, as civilization has advanced during the last centuries, so has likewise steadily advanced, especially in war on land, the distinction between the private individual belonging to a hostile country

Declaration,[71] distinction is a norm of customary international law.[72] Additional Protocol I provides a contemporary definition of the principle of distinction by stating:

> [I]n order to ensure respect for and protection of the civilian population and civilian objects, the Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives.[73]

Additional Protocol I further clarifies this legal obligation in regards to objects by requiring any attack — defined as any act of "violence against the adversary, whether in the offence or defence"[74] — to be "limited strictly to military objectives."[75] Military objectives are those "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."[76] This broad definitional framework allows for command discretion in interpretation. Ultimately, combatants must make judgments, often in very difficult and time-sensitive circumstances, in applying this definition. For example, when an object's "total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage"

and the hostile country itself, with its men in arms. The principle has been more and more acknowledged that the unarmed citizen is to be spared in person, property, and honor as much as the exigencies of war will admit.").

[71] 1868 St. Petersburg Declaration, *supra* note 60 ("[T]he only legitimate object which States should endeavor to accomplish during war is to weaken the military forces of the enemy . . . .").

[72] *E.g.*, Schmitt, *Autonomous Weapon Systems*, *supra* note 66, at 10; *see also* JEAN-MARIE HENCKAERTS & LOUISE DOSWALD-BECK, INTERNATIONAL COMMITTEE OF THE RED CROSS, CUSTOMARY INTERNATIONAL HUMANITARIAN LAW VOLUME I: RULES 25, 40 (2005).

[73] Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflict (Protocol I) art. 48, June 8, 1977, 1125 U.N.T.S. 3 [hereinafter AP I]. It is important to note that the United States has not ratified Protocol I or Protocol II but finds many portions of the protocols to be customary international law. *See generally* Michael J. Matheson, *Session One: The United States Position on the Relation of Customary International Law to the 1977 Protocols Additional to the 1949 Geneva Conventions*, 2 AM. U. J. INT'L L. & POL'Y 419 (1987).

[74] AP I, *supra* note 73, at art. 49(1). An "attack" includes both large and small-scale combat actions by either party to the hostilities. *See* COMMENTARY, *supra* note 69, at ¶ 1880; DINSTEIN, *supra* note 51, at 84.

[75] AP I, *supra* note 73, at art. 52(2). This definition is widely recognized as reflecting customary international law. *See* HENCKAERTS & DOSWALD-BECK, *supra* note 72, at 25.

[76] AP I, *supra* note 73, at art. 52(2).

depends upon the facts of a specific situation.[77] An otherwise civilian building may thus become targetable because it is being used by a party to the conflict. However, the protocol also provides clarity on what constitutes a "military objective" by requiring such objects to be only those that "by their nature, location, purpose, or use make an effective contribution to military action."[78]

Objects that by their nature make an effective contribution to military action include, but are not limited to, all those items directly used by armed forces such as: weapons, equipment, transports, fortifications, depots, buildings occupied by armed forces, staff headquarters, and communications facilities.[79] Other objects that may not have a military function may still directly contribute to military action simply due to their geography and location.[80] Natural land areas like beaches, mountain passes, and ridges or constructed items such as bridges or roads may therefore qualify as a military objective.[81] The future intended purpose of an object also determines whether it has an effective contribution to military action — for example, a civilian luxury liner that can easily transform into a method of troop transport.[82] Finally, the current use of a traditionally civilian object — like a hotel or church acting as headquarters for a military's staff — also determines if it is a military objective.[83]

---

[77] *Id.*; *see* LAURIE R. BLANK & GREGORY P. NOONE, INTERNATIONAL LAW AND ARMED CONFLICT: FUNDAMENTAL PRINCIPLES AND CONTEMPORARY CHALLENGES IN THE LAW OF WAR 399 (2013) (noting that a civilian object would not offer a definite military advantage at one moment but could if converted into a command post, a weapon storage facility, or a location to launch attacks). The reference to "military advantage" in the definition of military objective is positive expression of the broader concept of "military necessity." *See generally* Schmitt, *Autonomous Weapon Systems*, *supra* note 66, at 22.

[78] AP I, *supra* note 73, at art. 52(2); *see also* BLANK & NOONE, *supra* note 77, at 397 (discussing how "nature, location, use [and] purpose" are separate and definable criteria for determining a military objective).

[79] *See* COMMENTARY, *supra* note 69, at ¶ 2020.

[80] *See* BLANK & NOONE, *supra* note 77, at 398-99.

[81] *See* COMMENTARY, *supra* note 69, at ¶ 2021 ("[A] site which is of special importance for military operations in view of its location, either because it is a site that must be seized or because it is important to prevent the enemy from seizing it, or otherwise because it is a matter of forcing the enemy to retreat from it.").

[82] SOLIS, *supra* note 56, at 511-12. Professor Solis notes that converting luxury liners into troop transports was a regular practice during World War II and the Korean Conflict. *Id.* at 511. In fact, as late as 1982, during the United Kingdom-Argentina Falklands conflict, "the P&O Cruise Line's forty-five-thousand-ton *Canberra* was requisitioned by the British Ministry of Defense, hastily converted to troop use, and used to transport two thousand combatants to the Falklands." *Id.* at 511-12.

[83] *See* COMMENTARY, *supra* note 69, at ¶ 2022.

Many objects have dual military and civilian functions. Additionally, even in those circumstances where an object is exclusively a military objective, surrounding civilian objects may be at risk during targeting. Pursuant to the principle of proportionality,[84] parties to the conflict are obligated to minimize "collateral damage" or, in other words, the effects of the attack on the civilian population.[85] However, damage to civilian property does not necessarily indicate a violation of the principle of distinction.[86] Rather, launching an attack that may be expected to cause incidental loss of civilian life, injury to civilians, or damage to civilian objects is prohibited if the death, injury, or damage to civilian life and property is excessive in relation to the direct and concrete military advantaged gained.[87] For example, the presence of a soldier on leave cannot justify the destruction of an entire village. By contrast, if the destruction of a bridge is vitally important to the success of a military operation, it is understood that some nearby civilians' buildings may be hit in the attack of the bridge.[88] Similar to the definition of military objective, commanders have discretion in the proportionality analysis as the military advantage gained is circumstance-specific and the incidental loss to civilian life and property is typically only an estimate.[89] While this analysis is therefore always contextual, at a minimum the principle of proportionality acts as a protective threshold by ensuring the unintended civilian harm is not on a scale such that it is tantamount to being indiscriminate.[90]

---

[84] The principle of proportionality is a norm of customary international law. *See generally* HENCKAERTS & DOSWALD-BECK, *supra* note 72, at 46.

[85] *See* DINSTEIN, *supra* note 51, at 155.

[86] *See* SOLIS, *supra* note 56, at 292 (quoting Yoram Dinstein, *Discussion: Reasonable Military Commanders and Reasonable Civilians*, 78 INT'L L. STUD. 173, 219 (2002)) ("Nevertheless, the realistic goal is to minimize civilian casualties, not to eliminate them altogether. There is no way to eliminate civilian deaths and injuries due to collateral damage, mistake, accident and just sheer bad luck."). In fact, extensive civilian casualties or destruction of property is acceptable if it is not excessive in relation to the direct and concrete military advantage gained. *Id.* at 292-93 (discussing proportionality).

[87] *See* AP I, *supra* note 73, at arts. 51(5)(b), 57(2)(a)(iii). Other treaties express the principle of proportionality as well. *See, e.g.*, Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflict (Protocol II) art. 14, June 8, 1977, 1125 U.N.T.S. 313 [hereinafter AP II]; Rome Statute of the International Criminal Court, art. 8(2)(b)(iv), July 17, 1998, 2187 U.N.T.S. 90.

[88] *See* COMMENTARY, *supra* note 69, at ¶¶ 2213-14.

[89] *See* Schmitt, *Autonomous Weapon Systems*, *supra* note 66, at 24 (stating that the proportionality analysis is contextual).

[90] *See* Corn et al., *supra* note 51, at 182.

Further supplementing the principle of distinction is the well-understood customary international norm that "in the conduct of military operations, constant care shall be taken to spare the civilian population, civilians and civilian objects."[91] This mandate imposes, on both the attacking and defending parties in the hostilities, a number of precautionary legal obligations. For the attacking party, these obligations include: doing everything feasible[92] to identify military objectives and direct attacks only at those targets;[93] taking all feasible precautions in the choice of the means and methods of warfare;[94] refraining or canceling any attack that violates the principle of proportionality;[95] providing advanced warning to civilians if circumstances permit;[96] and targeting the military objective, when possible, that is "expected to cause the least danger to civilian lives and to civilian objects."[97] The defending party, for their part, must take feasible measures to protect the civilian population, individual civilians, and civilian objects from the dangers resulting from military operations.[98]

C. Specially Protected Objects — Works and Installations Containing Dangerous Forces

Certain types and classes of objects receive protections in addition to those provided by the general legal framework described above. A non-

[91] AP I, *supra* note 73, at art. 57(1); *see also* BOOTHBY, LAW OF TARGETING, *supra* note 52, at 119 (discussing how the general rules of precautions in the attack can reasonably be regarded as supplementing the principle of distinction). Precautions in the attack were first codified in Article 2 of the 1907 Hague IX Regulations. *See* Convention Between the United States and Other Powers Concerning Bombardment by Naval Forces in Time of War, art. 2, Oct. 18, 1907, 36 Stat. 2351. The obligation to take precautions in the attack is customary international law. *See* HENCKAERTS & DOSWALD-BECK, *supra* note 72, at 51.

[92] "Feasible" is that which is "practicable or practically possible, taking into account all circumstances ruling at the time, including humanitarian and military considerations." Protocol on Prohibitions or Restrictions on the Use of Mines, Booby-Traps and Other Devices (Protocol II), art. 3(10), as amended May 3, 1996, 2048 U.N.T.S. 93.

[93] *See* AP I, *supra* note 73, at art. 57(2)(a)(i).

[94] *See id.* at art. 57(2)(a)(ii); *see also* A. P. V. ROGERS, LAW ON THE BATTLEFIELD 96 (2d ed. 2004) (noting that the means and methods of warfare chosen must be likely to hit the target).

[95] *See* AP I, *supra* note 73, at arts. 57(2)(a)(iii), (b).

[96] *See id.* at art. 57(2)(c).

[97] *Id.* at art. 57(3).

[98] *See id.* at art. 58.

exhaustive list of examples includes medically-related objects,[99] the natural environment,[100] cultural property,[101] and objects indispensable to the survival of the civilian population.[102] However, of particular relevance to the potential targeting of critical infrastructure is the special protections provided for works and installations containing dangerous forces.

Additional Protocol I, Article 56 prohibits "dams, dykes and nuclear electrical generating stations" from being the "object of attack, even where these objects are military objectives, if such attack may cause the release of dangerous forces and consequent severe losses among the civilian population."[103] Further, the rule provides that other military objectives located at, or near, these works or installations "shall not be made the object of attack if such attack may cause the release of dangerous forces . . . and consequent severe losses among the civilian population."[104] The rule also requires attackers to take all practical precautions to avoid the release of the dangerous forces if the structure loses special status[105] and prohibits making dams, dykes, and nuclear electrical generating stations the object of reprisals.[106] Finally, although the rule appears largely focused on attacking forces, it also applies to military operations in the defense stating "[t]he Parties to the conflict shall endeavour to avoid locating any military objectives in the vicinity of the works or installations . . . ."[107]

As justification for these special protections, the Commentary to the rule offers several historical incidents where catastrophic collateral damage resulted from attacks on works or installations containing dangerous forces. For example, in 1938 Chinese Nationalists destroyed

[99] *See, e.g.*, Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, arts. 33-37, Aug. 12, 1949, 6 U.S.T. 3114, 75 U.N.T.S. 31.

[100] *See, e.g.*, AP I, *supra* note 73, at arts. 35(3), 55.

[101] *See, e.g.*, Convention for the Protection of Cultural Property in the Event of Armed Conflict, arts. 2-4, May 14, 1954, 249 U.N.T.S. 240.

[102] *See, e.g.*, AP I, *supra* note 73, at art. 54.

[103] *Id.* at art. 56(1). Similar protections also apply in a non-international armed conflict. *See* AP II, *supra* note 87, at art. 15.

[104] AP I, *supra* note 73, at art. 56(1).

[105] The terminology "special status" refers to heightened protections under the law of international armed conflict. As noted in the commentary to Article 56, "[i]t seemed appropriate to specify that in any attack directed against a dam, dyke or nuclear electrical generating station which had ceased to enjoy special protection, all other rules protecting the civilian population must be respected." COMMENTARY, *supra* note 69, at ¶ 2168.

[106] *See* AP I, *supra* note 73, at art. 56(4).

[107] *Id.* at art. 56(5).

the dykes of the Yellow River near Chang-Chow to stop advancing Japanese troops, resulting in extraordinary civilian death and property damage.[108] However, the protections described in the article are not absolute and are limited in two circumstances. First, these special protections only applies to dams, dykes, and nuclear electrical generating stations, which, if attacked, would release dangerous forces causing severe civilian losses.[109] Accordingly, if the structure is away from areas of civilian habitation, and is a military objective, there is no prohibition on such an attack.[110] Second, the special protections under the rule cease if the structure "is used for other than its normal function and in regular, significant and direct support of military operations and if such attack is the only feasible way to terminate such support."[111]

Article 56 is not without controversy. The United States categorically denied the applicability of the rule to its military operations.[112] Similarly, on ratification of Additional Protocol I, the United Kingdom stated it could not "undertake to grant absolute protection to installations which may contribute to the opposing party's war effort, or to the defenders of such installations" but would "take all due precautions in military operations" based on known facts.[113] France also agreed absolute protections for works or installations was not possible.[114] As a result, a more limited set of prohibitions on targeting works and installations containing dangerous forces is arguably also customary international law.[115]

---

[108] *See* COMMENTARY, *supra* note 69, at ¶ 2142. Other historic examples discussed in the Commentary include German troops flooding thousands of hectares of farmland in the Netherlands with seawater in 1944 and numerous deliberate attacks in 1943 against hydroelectric dams in Germany. *See id.* at ¶¶ 2142-43.

[109] *See* AP I, *supra* note 73, at art. 56(1).

[110] *See* DINSTEIN, *supra* note 51, at 174.

[111] AP I, *supra* note 73, at art. 56(2); *see also* DINSTEIN, *supra* note 51, at 174.

[112] *See* Matheson, *supra* note 73, at 427 ("[W]e do not support the provisions of [A]rticle 56, concerning dams, dykes, and nuclear power stations . . . ."). The United States stressed that the proportionality analysis was appropriate for assessing the legality of an attack against such works or installations. *See* BOOTHBY, LAW OF TARGETING, *supra* note 52, at 247 n.81. Whether this is still the position of the United States is unclear.

[113] BOOTHBY, LAW OF TARGETING, *supra* note 52, at 248; *see also* HENCKAERTS & DOSWALD-BECK, *supra* note 72, at 140.

[114] HENCKAERTS & DOSWALD-BECK, *supra* note 72, at 140.

[115] *See id.* at 139; *see also* TALLINN MANUAL 2.0, *supra* note 21, at 529. The International Group of Experts that drafted the Tallinn Manual generally agreed that neither Article 56 nor Additional Protocol II, Article 15, were customary international law. *See id.* The Tallinn authors therefore drafted a more limited rule to reflect customary international law than that found in the Additional Protocols by drawing from Rule 42 of the International Committee of the Red Cross's Customary

Regardless of the outcome of this debate, Article 56 provides a legal framework for considering how best to protect important objects.[116] Determining whether critical infrastructure requires heightened protections from cyber-attacks during an armed conflict depends on whether the existing law of targeting provides adequate legal safeguards. Application of the law of armed conflict's general principles and rules to critical infrastructure in cyberspace is therefore necessary to make this determination.

III. APPLYING THE EXISTING RULES TO CRITICAL INFRASTRUCTURE IN CYBERSPACE

Understanding how the existing law of targeting regulates cyber-attacks against critical infrastructure during an armed conflict is not merely an abstract academic pursuit. This exercise is of utmost importance as advanced States rely heavily on critical infrastructure to perform essential societal functions. Consequently, as the threat posed by cyber means and methods increases, so does the relevance of this analysis.[117]

A. Law of Armed Conflict Applies to Cyberspace

As a preliminary matter, it is important to establish that the law of armed conflict applies in cyberspace. In 2009, the NATO Cooperative Cyber Defence Centre of Excellence ("NATO CCD COE"), a cyber think tank in Tallinn, Estonia, convened a group of international law experts to develop a practical manual on cyber conflict.[118] This group of legal scholars and practitioners, referred to as the International Group of Experts, analyzed and then articulated how extant legal norms

International Humanitarian Law Study, which states "[p]articular care must be taken if works and installations containing dangerous forces, namely dams, dykes and nuclear electrical generating stations, and other installations located at or in their vicinity are attacked, in order to avoid the release of dangerous forces and consequent severe losses among the civilian population." *Id.* (citing HENCKAERTS & DOSWALD-BECK, *supra* note 72, at 139).

116 In fact, Article 56 appears to recognize the need for protecting future, unanticipated works or installations by including a provision urging the High Contracting Parties and the Parties to the conflict "to conclude further agreements among themselves to provide additional protections for objects containing dangerous forces." AP I, *supra* note 73, at art. 56(6).

117 For a comprehensive approach to emerging technology and the law of armed conflict, see generally THE IMPACT OF EMERGING TECHNOLOGIES ON THE LAW OF ARMED CONFLICT (Eric Talbot Jensen & Ronald T.P. Alcala eds., 2019).

118 *See* TALLINN MANUAL 2.0, *supra* note 21, at 1.

apply to cyber warfare.[119] Their efforts resulted in the *Tallinn Manual on International Law Applicable to Cyber Warfare* in 2013.[120] In its nearly 600 pages, the manual addresses vital issues spanning public international law and in particular the law governing cyber warfare. In light of the success of the first manual, the NATO CCD COE initiated a subsequent effort to enlarge the scope of coverage with an updated Tallinn Manual to include the international law governing cyber activities during peacetime. As part of the follow-on effort, the NATO CCD COE again assembled a group of international law experts, which led to the creation and publication of *Tallinn Manual 2.0* in February 2017. *Tallinn Manual 2.0* not only incorporated and updated the materials from the first *Tallinn Manual*, but also included coverage of peacetime international legal regimes and frameworks.[121] Importantly, the *Tallinn Manual 2.0* experts limited the manual to an objective restatement of the *lex lata* and avoided including statements reflecting the *lex ferenda*.[122]

Tallinn Manual 2.0 expressly states that the current law of armed conflict applies to cyberspace and cyber-attacks during armed conflict.[123] While, to date, there are no cyber-specific law of armed conflict treaties, the Martens Clause, found in the preamble to the 1899

---

[119] *See id.*; *see also* Jeremy Kirk, *Manual Examines How International Law Applies to Cyberwarfare*, CIO (Sept. 3, 2012, 7:00 AM), https://www.cio.com/article/2392610/manual-examines-how-international-law-applies-to-cyberwarfare.html [https://perma.cc/YEK5-SHUL] (noting that the Cooperative Cyber Defense Center of Excellence, which "assists NATO with technical and legal issues associated with cyberwarfare-related issues," created the Tallinn Manual to examine "existing international law that allows countries to legally use force against other nations, as well as laws governing the conduct of armed conflict").

[120] *See* TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE 1 (Michael N. Schmitt ed., 2013) [hereinafter TALLINN MANUAL 1.0].

[121] *See* TALLINN MANUAL 2.0, *supra* note 21, at 1.

[122] *See id.* at 3.

[123] *See id.* An "armed conflict" triggers the law of armed conflict. *See* ADVISORY SERV. ON INT'L HUMANITARIAN LAW, *supra* note 22 ("International humanitarian law applies only to [international or non-international] armed conflict; it does not cover internal tensions or disturbances such as isolated acts of violence. The law applies only once a conflict has begun, and then equally to all sides regardless of who started the fighting."). While there is not a conclusive definition of the term "armed conflict," it is generally understood to "exist[] whenever there is a resort to armed force between States or protracted armed violence between governmental authorities and organized armed groups or between such groups within a State." Prosecutor v. Tadi , Case No. IT-94-1-l, Decision on Defence Motion for Interlocutory Appeal on Jurisdiction, ¶ 70 (Int'l Crim. Trib. for the Former Yugoslavia Oct. 2, 1995).

Hague Convention (II),[124] reflects customary international law and remains applicable even in novel cyber situations.[125] Therefore, the lack of cyber-specific treaties does not equate to a legal lacuna regarding the application of the law of armed conflict to cyberspace and cyber-attacks[126] as the Martens Clause extends existing principles and rules to fill any gaps in legal regulations caused by emerging technologies and, specifically, cyber capabilities.

While the *Tallinn Manual 2.0* experts were unanimous in their conclusion that the law of armed conflict applies to both international and non-international armed conflicts,[127] this determination has recently come into question. In 2015, the United Nations General Assembly requested a body of experts to form a group officially titled the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, or more simply, the UN Group of Government Experts ("UN GGE"). The task of the UN GGE was to build upon the conclusions of four previous experts' reports in order to promote common understandings on various technology related matters including "how international law applies to the use of information and communications technologies by States."[128] Despite adopting an uncontroversial

---

[124] *See* Preamble, Convention Between the United States and Certain Powers, with Respect to the Laws and Customs of War on Land, July 29, 1899, 32 Stat. 1803 [hereinafter Hague Convention II]. Specifically, the Martens Clause states:

> Until a more complete code of the laws of war is issued, the High Contracting Parties think it right to declare that in cases not included in the Regulations adopted by them, populations and belligerents remain under the protection and empire of the principles of international law, as they result from the usages established between civilized nations, from the laws of humanity and the requirements of the public conscience.

Id.

[125] The Martens Clause is often invoked in the interpretation of law of armed conflict treaties "both to rule out that what is not expressly prohibited is permitted and as a presumption that favours humanitarian considerations whenever doubts exist on the meaning of certain provisions." MARCO ROSCINI, CYBER OPERATIONS AND THE USE OF FORCE IN INTERNATIONAL LAW 22 (2014).

[126] The Martens Clause is the subject of a great deal of controversy with some arguing that it represents an enforceable legal principle and others arguing the clause is more general guidance. For a more detailed discussion, see Dave Wallace & Shane R. Reeves, *Modern Weapons and the Law of Armed Conflict*, *in* U.S. MILITARY OPERATIONS: LAW, POLICY, AND PRACTICE 41, 62-63 (Geoffrey S. Corn et al. eds., 2016).

[127] TALLINN MANUAL 2.0, *supra* note 21, at 375.

[128] G.A. Res. 70/237, Developments in the Field of Information and Telecommunications in the Context of International Security (Dec. 23, 2015).

approach to the applicability of international law to cyberspace, a number of States rejected the final report in 2017.[129]

By rejecting the report, some legal questions remain unsettled.[130] However, the States' non-concurrence with the report was seemingly more of a political decision than a rejection of the understanding that international law applies in cyberspace.[131] In fact, whether the law of armed conflict applies in the cyber context is seemingly a resolved issue "[s]ince no international lawyer can . . . deny their applicability to cyber activities, [so] the failure of the GGE can only be interpreted as the intentional politicization in the cyber context of well-accepted international law norms."[132]

B. What Is a "Cyber Armed Attack?"

Since the law of armed conflict applies fully to cyberspace, the meaning of "cyber-attack" is critical it serves as the basis for numerous limitations and prohibitions under the international law.[133] Rule 92 of *Tallinn Manual 2.0* provides that a cyber-attack is "a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects," whereas

---

[129] *See* Michael Schmitt & Liis Vihul, *International Cyber Law Politicized: The UN GGE's Failure to Advance Cyber Norms*, JUST SECURITY (June 30, 2017), https://www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms [https://perma.cc/337F-DD8V]. While only Cuba issued a formal declaration of non-concurrence with the report, Russia and China also reportedly rejected the group's final product. *See id.*

[130] *See id.* ("The real legal challenge lies in determining when and how the aforementioned rights and legal regimes apply in the unique cyber context, questions Russia, China and the other recalcitrant States have deftly sidestepped.").

[131] *See id.* (noting that "[r]educed to basics, the States concerned have put forward what are essentially political arguments that make little legal sense"). The United States has expressly stated that international law applies in cyberspace. *See* THE WHITE HOUSE, INTERNATIONAL STRATEGY FOR CYBERSPACE: PROSPERITY, SECURITY, AND OPENNESS IN A NETWORKED WORLD 9 (2011) ("The development of norms for state conduct in cyberspace does not require a reinvention of customary international law, nor does it render existing norms obsolete. Long-standing international norms guiding state behavior — in times of peace and conflict — also apply in cyberspace."); *see also* Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, ¶ 19, U.N. Doc. A/68/98 (June 24, 2013) (noting that the United States, as well as other important States such as China and Russia, agreed that "[i]nternational law, and in particular the Charter of the United Nations, is applicable" to cyberspace).

[132] Schmitt & Vihul, *supra* note 129.

[133] *See* Schmitt, *Law of Cyber Warfare*, *supra* note 29, at 294. Again, an "attack" is defined as an act of "violence against the adversary, whether in the offence or in defence." AP I, *supra* note 73, at art. 49(1).

non-violent operations do not qualify as an attack.[134] However, "[c]yber operations have complicated matters in that they can be highly useful militarily without generating destructive or injurious effects."[135] Therefore,"[t]he violence must be understood in terms of the consequences of the act rather than the act itself; hence, violent acts may include cyber (computer network) attacks leading to mayhem and destruction."[136]

For example, a cyber operation against an electrical grid or a hydro-electrical plant that results in violent consequences is a cyber-attack,[137] and, as such, is subject to the law of targeting. In contrast, an act of cyber espionage having no violent effects is not a cyber-attack and, therefore, the principle of distinction and its supplementing provisions do not regulate that behavior. Yet, there is difficulty in determining whether the concept of "attack" extends to certain nondestructive or non-injurious cyber operations such as altering or destroying data.[138] The majority of the experts behind *Tallinn Manual 2.0* took the position that, under the current state of the law, the concept of "object" is not interpreted to include something as intangible as "data."[139] Noting that "data" does not fall under the ordinary meaning of the word "object" nor comports with how the Commentary to Additional Protocol I defines the term,[140] the majority of the experts were not willing to extend the concept of "attack" to damaging or destroying data. However, this position seems untenable going forward as Professor Michael N. Schmitt notes:

> Given the pervasive importance of cyber activities, an interpretation that limits the notion of attacks to acts generating physical effects cannot possibly survive. Suggestions that civilian activities may lawfully be seriously disrupted or that important data can be altered or destroyed because there is no resulting physical damage or injury will surely collide with

134 TALLINN MANUAL 2.0, *supra* note 21, at 415.

135 Schmitt, *Law of Cyber Warfare*, *supra* note 29, at 294.

136 DINSTEIN, *supra* note 51, at 84; *see also* TALLINN MANUAL 2.0, *supra* note 21, at 415.

137 *See* TALLINN MANUAL 2.0, *supra* note 21, at 416.

138 *See id.* at 437.

139 *Id.*

140 *See* COMMENTARY, *supra* note 69, at ¶¶ 2007-08 (noting that the term "object" means something "visible and tangible" that can be "placed before the eyes, or presented to the sight or other sense, an individual thing seen, or perceived, or that may be seen or perceived; a material thing").

> future assessments of the military necessity/humanitarian considerations balance.[141]

At a minimum, it appears that a cyber operation that interferes "with the functionality of an object" necessitating "repair of the target cyber infrastructure" qualifies as a cyber-attack.[142] Yet, while the existing law may limit a cyber-attack to those events causing physical harm,[143] it is worth again noting that any cyber-attack on critical infrastructure could potentially result in extreme, unanticipated consequences.[144] Deleting, corrupting, altering, or otherwise disrupting the computer network supporting critical infrastructure may result in the destruction or incapacitation of the structure or facility.[145] The effects of such an operation are not limited to simply causing damage to the computer networks of a given facility but may extend to large numbers of people through the loss of, for example, electrical power or water.[146] While physical damage to property, loss of life, and injury to persons may not be the intended purpose of the cyber-attack that targets critical infrastructure, this could be the result.[147] Therefore, while *de minimis* damage to critical infrastructure may not meet the cyber-attack definitional threshold, considering the expected secondary and tertiary effects of any such operation is necessary in applying the law of armed conflict.

C. The Law of Targeting Applied to Cyber-Attacks Against Critical Infrastructure During Armed Conflict

A cyber-attack occurring against critical infrastructure during an armed conflict triggers the law of targeting as it specifically relates to objects and, consequently, any concomitant protections.[148] The principle of distinction clearly prohibits a cyber-attack on critical

---

141 Schmitt, *Law of Cyber Warfare*, *supra* note 29, at 295-96.

142 *Id.* at 295 (citing TALLINN MANUAL 1.0, *supra* note 120, at 93).

143 The likelihood that the concept of "cyber-attack" remains limited to causing physical harm to person and/or tangible objects is unlikely to remain static. Most likely, the notion of cyber-attack will expand to "include interference with essential civilian functions." *Id.* at 296. For a discussion on the difficulty in expanding the definition of "cyber-attack," see *id.*

144 *See supra* Part II (highlighting the potential devastating consequences of an attack on critical infrastructure).

145 *See* ROSCINI, *supra* note 125, at 52.

146 *See id.* at 52-53.

147 *See id.* at 53.

148 *See supra* Part III (highlighting what triggers the law of targeting).

infrastructure exclusively used for a civilian purpose.[149] However, critical infrastructure is generally dual use in nature — meaning it has both a military and civilian function — and therefore qualifies as military objective.[150] For example,

> military communications occur in part across cables and other media that are also used for civilian traffic. Weapons often rely on data generated by the Global Positioning Satellite (GPS) system, which serves civilian purposes such as navigation. Social media like Facebook and Twitter have been widely used during recent conflicts to transmit militarily important information. Militaries are also increasingly turning to 'off the shelf' equipment like commercial computer systems for their forces, thereby qualifying the factories which produce the products as military objectives.[151]

Certainly, if the military and civilian functions are distinguishable in dual-use critical infrastructure, any cyber-attack may only target the military function.[152] Still, most critical infrastructure is interconnected and interdependent, making such fine discernments extremely difficult. As a result, protections for critical infrastructure from a cyber-attack occurring during an armed conflict are primarily through the principle of proportionality and the requirement to take precautions in the attack.[153]

"[T]he principle of proportionality allows, in effect, an attacker to conduct an attack in the knowledge"[154] that civilian objects will be damaged or destroyed assuming such loss is incidental and not "excessive in relation to the concrete and direct military advantage

---

[149] *See* AP I, *supra* note 73, at art. 48; *see also* TALLINN MANUAL 2.0, *supra* note 21, at 420-21.

[150] *See* AP I, *supra* note 73, at art. 52(2); *see also* Schmitt, *Law of Cyber Warfare*, *supra* note 29, at 298 ("The extent of military use is irrelevant; so long as the object is being employed militarily, it qualifies as a military object subject to attack." (citing TALLINN MANUAL 1.0, *supra* note 120, at 112)).

[151] Schmitt, *Law of Cyber Warfare*, *supra* note 29, at 298.

[152] *See* AP I, *supra* note 73, at art. 51(5)(a) (defining an indiscriminate attack as "an attack by bombardment by any methods or means which treats as a single military objective a number of clearly separated and distinct military objectives located in a city, town, village or other area containing a similar concentration of civilians or civilian objects"). The Tallinn Manual 2.0 updates and operationalizes this provision for cyber-attacks in Rule 112. *See* TALLINN MANUAL 2.0, *supra* note 21, at 469-70.

[153] *See supra* Part III.B. (discussing proportionality).

[154] Ian Henderson & Kate Reece, *Proportionality Under International Humanitarian Law: The "Reasonable Military Commander" Standard and Reverberating Effects,* 51 VAND. J. TRANSNAT'L L. 835, 854 (2018).

anticipated."[155] While calculating the expected collateral damage from a cyber-attack on critical infrastructure is difficult,[156] the importance of these assets to ongoing military operations[157] makes the anticipated "concrete and direct military advantage" gained from such an attack significant.[158] Further, those planning or approving a cyber-attack against critical infrastructure have discretion as terms like "expected," "excessive," and "anticipated" that are embedded within the proportionality principle allow for a "fairly broad margin of judgment."[159] Future applications of the principle of proportionality may become more difficult for those conducting cyber-attacks as "[t]he notion of damage in the proportionality context will probably expand beyond a strict limitation to physical effects" and the term "object" may include a broader understanding.[160] However, as currently applied, the proportionality principle legally allows for, if necessary, extensive collateral damage from a cyber-attack against critical infrastructure during armed conflict.[161] In other words, as long as such damage remains below the "excessive" threshold there is no prohibition against

[155] TALLINN MANUAL 2.0, *supra* note 21, at 470.

[156] A cyber-attack may cause "what have been termed 'reverberating,' 'knock-on,' or 'indirect' effects." Henderson & Reece, *supra* note 154, at 847; *see also* TALLINN MANUAL 2.0, *supra* note 21, at 472 ("Collateral damage can consist of both direct and indirect effects."). However, the proportionality analysis considers only expected indirect effects in contrast to those that are remote possibilities. *See id.* at 475 ("The attacker either reasonably expects it or the possibility of collateral damage is merely speculative, in which case it would not be considered in assessing proportionality."). For a more detailed discussion on the difference between "expected" and "remote" indirect effects, see Henderson & Reece, *supra* note 154, at 846-54.

[157] *See supra* Part II (discussing the general importance of critical infrastructure).

[158] *See* AP I, *supra* note 73, at art. 51(5)(b).

[159] *See* COMMENTARY, *supra* note 69, at ¶ 2210. Of course, a commander must be "reasonable" when making a targeting decision. *See* TALLINN MANUAL 2.0, *supra* note 21, at 475 (citing Prosecutor v. Gali , Case No. IT-98-29-T, Judgement and Opinion, ¶ 58, (Int'l Crim. Trib. for the Former Yugoslavia Dec. 5, 2003) ("In determining whether an attack was proportionate, it is necessary to examine whether a reasonably well-informed person in the circumstances of the actual perpetrator, making reasonable use of the information available to him or her, could have expected excessive civilian casualties to result from the attack.")). *See generally* Bill, *supra* note 57 (discussing the Rendulic Rule); Henderson & Reece, *supra* note 154, at 855 (arguing that the "appropriate standard for assessing a decision on the proportionality of attack is that of a 'reasonable military commander'").

[160] *See* Schmitt, *Law of Cyber Warfare*, *supra* note 29, at 297.

[161] *See* TALLINN MANUAL 2.0, *supra* note 21, at 473 ("[T]he majority of the International Group of Experts took the position that extensive collateral damage may be legal if the anticipated concrete and direct military advantage is sufficiently great.").

a cyber-attack against critical infrastructure functioning as a military objective.

Those executing a cyber-attack against critical infrastructure are also required to "be continuously sensitive to the effects of their activities on the civilian population and civilian objects, and to seek to avoid any unnecessary effects thereon."[162] Yet, similar to the principle of proportionality, in application the constant care obligation will most likely not prohibit a cyber-attack against critical infrastructure. The precautionary legal obligations — whether requiring a cyber-attacker to do everything feasible to verify the critical infrastructure is a military objective[163] or to take all feasible precautions in the choice of the cyber means and methods intended for the attack[164] — provide the decision-maker ample discretion to go forward with a cyber-attack. In fact, the term "feasible" is widely accepted as that which is "practicable or practically possible, taking into account all circumstances ruling at the time, including humanitarian and military considerations."[165] The other express precautionary provisions also contain sufficiently ambiguous language to allow for a cyber-attack.[166] Consequently, the requirement to take precautions in the attack may shape how the cyber-attack occurs, but will not legally prohibit such action.[167]

Given the nature of critical infrastructure and the possible catastrophic consequences associated with cyber-attacks against such objects, the general protections provided by the law of targeting are insufficient.[168] Logically, this would seem to trigger the special

---

[162] *Id.* at 477 (citing U.K. MINISTRY OF DEFENCE, THE JOINT SERVICE MANUAL OF THE LAW OF ARMED CONFLICT ¶ 5.32.1 (2004)).

[163] *See* AP I, *supra* note 73, at art. 57(2)(a)(i).

[164] *Id.* at art. 57(2)(a)(ii).

[165] *E.g.*, Protocol on Prohibitions or Restrictions on the Use of Incendiary Weapons (Protocol III), art. 1(5), Oct. 10, 1980, 1342 U.N.T.S. 171.

[166] For example, the attacker must provide advance warning to civilians if "circumstances permit," AP I, *supra* note 73, at art. 57(2)(c), and, when possible, only target the military objective that is "expected to cause the least danger to civilian lives and to civilian objects." *Id.* at art. 57(3).

[167] *See* Henderson & Reece, *supra* note 154, at 854 (noting that even if "all the appropriate precautions are taken, there will be some circumstances in which . . . civilian objects remain in danger of incidental harm from an attack").

[168] *See, e.g.*, Rob Taylor & Mayumi Negishi, *U.S. Allies Raise New Security Worries About China's Huawei*, WALL ST. J. (Dec. 7, 2018, 12:54 PM), https://www.wsj.com/articles/water-electricity-would-be-at-risk-in-attacks-on-5g-networks-australian-intelligence-chief-says-1544182836 [https://perma.cc/V6BQ-A6NJ]. "The head of Australia's top military cyber defense agency, Mike Burgess, said Chinese companies were blocked from the rollout of 5G mobile-phone capabilities in August because the new technology" would threaten critical infrastructure. *Id.* Mr. Burgess clarified the

protections extended for particular objects found within the law of armed conflict.[169] More specifically, the extra-legal safeguards provided for works and installations containing dangerous forces found in Additional Protocol I, Article 56[170] are relevant to regulating cyber-attacks during armed conflicts. Unfortunately, these provisions are limited to a narrow class of objects and do not comprehensively guard a State's entire critical infrastructure.[171] These provisions are therefore most helpful if viewed as a blueprint for how the law can evolve to provide heightened protections against cyber-attacks for critical infrastructure during armed conflicts.

IV. PROTECTING CRITICAL INFRASTRUCTURE IN AN ERA OF CYBER WARFARE

It is increasingly "inconceivable that the extant law of cyber warfare, which responds to cyber operations that are still in their relative technological infancy, will survive intact" in today's technological age.[172] This is especially true as "cyber activities become ever more central to the functioning of modern societies, the law is likely to adapt by affording them greater protection."[173] The trend therefore, is towards greater protections for those assets, including critical infrastructure, that are essential to civilian activities.[174] However, how these protections evolve, especially during an armed conflict, is currently unknown.[175]

reasoning by stating, "[i]f the 5G network of the future isn't there, there's a good chance electricity supply might be interrupted, water supply might be interrupted, the financial sector or elements of it might impacted." *Id.* Similarly, Japan is taking steps to lower the cyber-infiltration risk of its government agencies and critical infrastructure. *See id.*

169 *See supra* notes 103–111 and accompanying text (discussing the law of targeting's special protection provisions).

170 *See* AP I, *supra* note 73, at art. 56. Additional Protocol II, Article 15 offers a counterpart for these provisions for a non-international armed conflict. *See* AP II, *supra* note 87, at art. 15. The special protections of objects indispensable to the survival of the civilian population may also be salient when exploring the idea of how best to provide additional legal safeguards for critical infrastructure. *See* AP I, *supra* note 73, at art. 54.

171 For example, the special protections for dams, dykes, and nuclear electrical generating stations would only insulate a minor portion of the United States' critical infrastructure. *See supra* notes 28, 30 and accompanying text (listing the sixteen critical infrastructure sectors designated by the United States).

172 Schmitt, *Law of Cyber Warfare*, *supra* note 29, at 271.

173 *Id.* at 299.

174 *See id.* at 296-99.

175 *See id.* at 296.

The legal framework contained in Additional Protocol I, Article 56 for protecting particularly important objects offers a possible solution to this problem. The special protections outlined in Article 56 expressly cover dams, dykes, and nuclear electrical generating stations.[176] These objects, a subset of any State's critical infrastructure, receive special protections because of the potentially catastrophic consequences of an attack. In contemporary warfare, a cyber-attack on critical infrastructure, whether it be a health care system, power grid, or transportation network, has the same possible devastating effects. Therefore, developing a legal provision similar to Article 56, albeit with broader understanding of what is a protected object seems to be a necessary expansion in this era of cyber warfare.

Perhaps more importantly, Additional Protocol I, Articles 56 provides a workable template for addressing cyber-attacks against critical infrastructure during armed conflict because of its pragmatic approach to targeting. While the extent of the protections described in Article 56 are debatable,[177] it is unquestioned that the article strives to strike the delicate balance between military necessity and humanitarian considerations required for a workable law of armed conflict legal provision.[178] For example, the article does not absolutely ban an attack on dams, dykes, and nuclear electrical generating stations but rather links a prohibition to attacks that "may cause the release of dangerous forces and consequent severe losses among the civilian population."[179] Moreover, the special protections afforded under Article 56 cease under specified conditions while also placing duties and obligations on both the attacker and the defender of the critical infrastructure.[180]

Given the operational reasons for targeting critical infrastructure, any future legal provision must address the military necessity-humanity balance. Otherwise, if viewed as less about fixing "the technical limits at which the necessities of war ought to yield to the requirements of humanity,"[181] and more about restricting all cyber-attacks on critical infrastructure,[182] the provision risks being ineffectual and ignored.

---

[176] *See* AP I, *supra* note 73, at art. 56(2).

[177] *See supra* notes 112–115 and accompanying text (noting the debate over Article 56 customary status and applicability).

[178] *See supra* Part III.A–B (discussing the military necessity-humanity balance).

[179] AP I, *supra* note 73, at art. 56(1).

[180] *See id.* at art. 56(2).

[181] 1868 St. Petersburg Declaration, *supra* note 61.

[182] *See* Reeves & Thurnher, *supra* note 57, at 12 ("It is incumbent upon states to maintain the balance between military necessity and humanity, as the primacy of the Law of Armed Conflict is dependent upon this equilibrium.").

Therefore, any new norm must look to Article 56 as a model for how to weigh military necessity with the dictates of humanitarian aims in order to be an effective regulatory provision. While States may resist joining a cyber-specific treaty protecting critical infrastructure during armed conflict, there may be incentives for States to sign and ratify such a treaty, tempered by a realistic skepticism that pervades compliance with and enforcement of the law of armed conflict generally.

First, States have an enlightened self-interest in protecting their own critical infrastructure. Given the increased capability of States to use digital combat power offensively, the vulnerabilities of and threats to advanced States' critical infrastructure are outpacing their ability to defend their networked computer systems.[183] A cyber-specific treaty establishing norms of behavior for protecting critical infrastructure during armed conflict is not and will never be a panacea. But, such an international agreement would be underpinned by notions of reciprocity. Once States bind themselves to such a treaty, the continued force of that treaty could be contingent on reciprocal observation by other States.[184] Notwithstanding the challenges associated with attribution in the cyber domain, if a State is found to be abusing the treaty, the attacking State would risk losing the protections associated with entering into the treaty.

A second, and related reason is that, at a minimum, such a cyber-specific treaty provides a special emphasis on the protection of critical infrastructure. As a general matter, civilian objects are protected under the law of armed conflict. There are some objects that receive special or heightened protections under the law of armed conflict "because of their particular importance for the protection of victims of armed conflicts, the civilian population or mankind in general or because of their particular vulnerability to destruction and damage in times of armed conflict."[185] In that regard, critical infrastructure is like other types of objects that the law of armed conflict identifies for heightened protections such as cultural property, medical facilitates, the natural environment and, most specifically, works or installations containing dangerous forces as represented by Additional Protocol I, Article 56.

---

[183] *See, e.g.*, DAVID E. SANGER, THE PERFECT WEAPON: WAR, SABOTAGE, AND FEAR IN THE CYBER AGE 300-01 (2018) (discussing the actions of the United States and other nations to defend their networked computer systems from a potential Chinese threat).

[184] Sean Watts, *Reciprocity and the Law of War*, 50 HARV. INT'L L. REV. 365, 375 (2009).

[185] *What Objects Are Specially Protected Under IHL?*, INT'L COMM. RED CROSS BLOG (Aug. 14, 2017), https://blogs.icrc.org/ilot/2017/08/14/objects-specially-protected-ihl/ [https://perma.cc/8YJW-EDF3].

Finally, adopting narrowly scoped international agreements to avoid potentially catastrophic consequences of armed conflict is not without precedent. For example, the 1976 *Convention on the Prohibition of Military or Any Other Hostile Use of Environmental Modification Techniques* ("ENMOD Convention") prohibits the use of "environmental modification techniques having widespread, long-lasting or severe effects as the means of destruction, damage or injury to any other State Party."[186] The ENMOD Convention defines "environmental modification techniques" as "any technique for changing — through the deliberate manipulation of natural processes — the dynamics, composition or structure of the Earth, including its biota, lithosphere, hydrosphere and atmosphere, or of outer space."[187] The ENMOD Convention was negotiated during a period of heightened international concern about the protection of the environment during armed conflict.[188] Namely, by the 1970s, the international community became increasingly aware that the toll of modern armed conflicts went far beyond human suffering and damage to physical property. It also led to extensive destruction and degradation to the natural environment.[189] Most notably, the widespread use of the defoliant Agent Orange during the Vietnam War resulted in environmental contamination and related human suffering and led to significant international criticism and concern.[190] The roots of the ENMOD Convention represent a reaction to State parties using environmental modification techniques as weapons of war. Some commentators have referred to these means and methods as "geophysical warfare."[191] Such environmental modification techniques include, but are not limited to, provoking earthquakes, tsunamis or changing weather patterns.[192]

Like the 1976 ENMOD Convention, a cyber-specific treaty protecting critical infrastructure would represent a meaningful and realistic effort

---

[186] *See* Convention on the Prohibition of Military or Any Other Hostile Use of Environmental Modification Techniques, art. I, Dec. 10, 1976, 1108 U.N.T.S. 151 [hereinafter ENMOD Convention]. The treaty is commonly referred to as the "ENMOD Convention." *See, e.g.*, *1976 Convention on the Prohibition of Military or any Hostile Use of Environmental Modification Techniques*, INT'L COMM. RED CROSS (Jan. 2003), https://www.icrc.org/en/download/file/1055/1976-enmod-icrc-factsheet.pdf.

[187] ENMOD Convention, *supra* note 186, at art. II.

[188] *See* ROBERTS & GUELFF, *supra* note 60, at 407.

[189] *See* U.N. ENV'T PROGRAMME, PROTECTING THE ENVIRONMENT DURING ARMED CONFLICT: AN INVENTORY AND ANALYSIS OF INTERNATIONAL LAW 8 (2009).

[190] *See* KAREN HULME, WAR TORN ENVIRONMENT: INTERPRETING THE LEGAL THRESHOLD 5-6 (2004).

[191] *See* U.N. ENV'T PROGRAMME, *supra* note 189, at 12.

[192] *Id.*

by States to reassert themselves in shaping the normative infrastructure of the law of armed conflict in response to an emerging technology that could cripple the backbone of modern societies — critical infrastructure. Similar to the effects of a disaster like starting earthquakes or creating hurricanes, cyber-attacks against a State's critical infrastructure will precipitate reverberating negative consequences that will permeate throughout that society. Intuitively, the more advanced and interconnected a State, the more devastating the effects will be. To complete the analogy between the ENMOD Convention and a cyber-specific treaty protecting critical infrastructure, it is reasonable to conclude that for both types of attacks — that is, those involving environmental modification techniques and those involving cyber capabilities — the outcomes simply cannot be predicted and controlled. For example, if a belligerent party creates a hurricane that hits Florida, the consequences may vary considerably depending on its strength and where it precisely lands. Likewise, a cyber-attack against a power grid or nuclear power plant could create many unforeseeable and catastrophic effects.

CONCLUSION

In October 2012, in a speech at the Intrepid Sea, Air & Space Museum in New York, United States Secretary of Defense Leon E. Panetta sounded an alarm that the United States was increasingly vulnerable to a "cyber-Pearl Harbor" that could dismantle the nation's critical infrastructure, including power grids, transportation systems, and financial networks.[193] According to Secretary Panetta, the most destructive possibilities involve hostile parties launching cyber operations against multiple critical infrastructure targets simultaneously in concert with a conventional attack.[194] Secretary Panetta's warning is not exclusive to the United States, but applies to any advanced State.

Therefore, the urgent need to protect critical infrastructure from cyber-attacks during armed conflict appears to provide an opportunity for the creation of the first cyber-specific law of armed conflict treaty. This treaty, built upon the legal blueprint found in Additional Protocol I, Article 56, would offer special protections to critical infrastructure from cyber-attacks during an armed conflict. Of course, promulgating a

[193] *See* Elisabeth Bumiller & Thom Shanker, *Panetta Warns of Dire Threat of Cyberattack on U.S.*, N.Y. TIMES (Oct. 11, 2012), https://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html [https://perma.cc/32UD-5N3U].

[194] *See id.*

new treaty is difficult. For example, even the definition of "critical infrastructure" would likely be a controversial topic requiring significant deliberation.[195] Yet, the very real threat to these assets during an armed conflict, coupled with the common cause shared by advanced States to protect critical infrastructure may provide the incentive necessary to develop a new conventional norm. Otherwise, States are left with the law of targeting's basic protections which, increasingly, are inadequate for protecting assets of such significant importance.

[195] Creation of a new conventional norm is the exclusive responsibility of States. *See* Schmitt, *Military Necessity*, *supra* note 65, at 799 (highlighting that only States can "reject, revise, or supplement" the Law of Armed Conflict or "craft new norms").

Tethering the Law of Armed Conflict to Operational Practice: "Organized Armed Group" Membership in the Age of ISIS

E. Corrie Westbrook Mack* & Shane R. Reeves**

DOI: https://doi.org/10.15779/Z38JW86N2M

* Lieutenant Colonel E. Corrie Westbrook Mack serves in the United States Air Force Judge Advocate General Corps and is currently stationed at the Headquarters, Air Force, Administrative Law Directorate at the Pentagon, Washington, District of Columbia.

** Lieutenant Colonel Shane Reeves is an Associate Professor and Deputy Head, Department of Law at the United States Military Academy.

The views expressed here are personal views and do not necessarily reflect those of the Department of Defense, the United States Army, the United States Military Academy, or any other department or agency of the United States Government. The analysis presented stems from academic research of publicly available resources, not from protected operational information.

INTRODUCTION

It is mid-June 2017 and the United States continues its long campaign in Syria and Iraq against the powerful non-State actor known as ISIS.[1] The war is going badly for ISIS as their greatest prize in Iraq, the large city of Mosul, is on the verge of being re-taken by the Iraqi military.[2] In an attempt to escape being trapped in Mosul, ISIS members are fleeing west towards Raqqah, Syria—the *de facto* capital of their so-called "caliphate."[3]

---

[1] The fact that the United States is currently involved in combat in Syria against ISIS is indisputable. *See* Christopher M. Blanchard and Carla E. Humud, *The Islamic State and U.S. Policy*, CRS REPORT 7-5700, R43612, 2 (Feb. 2017), https://fas.org/sgp/crs/mideast/R43612.pdf. Noting:

> the Islamic State (IS, aka the Islamic State of Iraq and the Levant, ISIL/ISIS, or the Arabic acronym Da'esh) is a transnational Sunni Islamist insurgent and terrorist group that controls large areas of Iraq and Syria, has affiliates in several other countries, has attracted a network of global supporters, and disrupts international security with its campaigns of violence and terrorism.

Id.

[2] Mosul was re-taken by Iraqi forces on 10 July 2017. *See* John Bacon, *Iraqi forces have fully retaken Mosul, U.S. backed coalition confirms*, USA TODAY (July 10, 2017), https://www.usatoday.com/story/news/world/2017/07/10/iraqi-forces-have-retaken-mosul-u-s-backed-coalition-confirms/465022001/.

[3] *See, e.g.*, Owen Holdaway, *On the Ground in Raqqa, Capital of Islamic State's Caliphate*, THE

The following hypothetical is illustrative of a likely scenario faced by the United States and coalition forces. As the ISIS exodus towards Raqqah is ongoing, the United States receives intelligence that a senior ISIS Military Commander, one they have been pursuing for the last two years, will be traveling the next day in a white car from Mosul to Raqqah. This ISIS Commander is known to be actively directing combat actions against the U.S. and Coalition Forces, Iraqi and Syrian government officials, and most troubling, at civilians who show resistance to ISIS. The source of the intelligence, who has proven to be extremely reliable in the past, has also shared that the ISIS Commander severely limits his travel in vehicles to minimize his risk of being targeted by U.S. aircraft. Additionally, tracking the ISIS Commander has become difficult as he has taken to giving orders to his subordinates in clandestine ways, primarily through encrypted phone messages which the U.S. has not yet unlocked. Thus, the ISIS Commander's decision to travel presents an extraordinary opportunity for the U.S. and Coalition Forces.[4]

But there is a complication. During the planning process, the U.S. receives additional intelligence that there will be a second white car traveling with the ISIS Commander driven by his brother. While the U.S. does not have extensive information on the brother, they do know that he identifies himself on social media as an ISIS member who has pledged an oath of loyalty to the group and its leader, Abu Bakr al Baghdadi. Further, he is known as one of the "public faces" of ISIS as he regularly makes videos advertising the group's violent efforts to establish the caliphate and highlighting their most recent military exploits. However, aside from this information, there are no indications that the brother actually carries out hostile activities in support of ISIS. With the window for a strike approaching, and with no way of knowing who is in each car, the planning cell must quickly decide whether to call off the strike or target both vehicles.

Although the above scenario is fictional,[5] the targeting dilemma presented is real. While most agree that status-based targeting of organized armed groups (OAG) in a non-international armed conflict (NIAC) is permissible,[6] what

JERUSALEM POST (Oct. 9, 2017), http://www.jpost.com/Middle-East/ISIS-Threat/On-the-ground-in-Raqqa-capital-of-Islamic-States-caliphate-507014.

[4] On September 10th, 2014, President Obama announced that combat efforts in Iraq and Syria would be joined by a Coalition of over 60 nations, providing various means of support to the combat effort. *See* Kathleen McInnis, *Coalition Contributions to Countering the Islamic State*, CRS REPORT R44135, 24 (Aug. 2016), https://fas.org/sgp/crs/natsec/R44135.pdf.

[5] If there are any similarities between this scenario and actual operations in Syria, they are coincidental.

[6] *See, e.g.*, U.S. DEPARTMENT OF DEFENSE, LAW OF WAR MANUAL ¶ 5.8.3 (2016) [hereinafter DOD LAW OF WAR MANUAL] ("Like members of an enemy State's armed forces, individuals who are formally or functionally part of a non-State armed group engaged in hostilities may be made the object of attack because they likewise share in their group's hostile intent" (*citing* Al-Adahi v. Obama, 613 F. 3d 1102, 1108 (D.C. Cir. 2010)); INTERNATIONAL COMMITTEE OF THE RED CROSS, INTERPRETIVE GUIDANCE ON THE NOTION OF DIRECT PARTICIPATION IN HOSTILITIES UNDER INTERNATIONAL HUMANITARIAN LAW 7, at 27–28 (Nils Melzer ed., 2009), http://www.icrc.org/eng/assets/files/other/icrc-002-0990.pdf [hereinafter ICRC INTERPRETIVE GUIDANCE] (discussing how members of organized armed groups in a non-international armed conflict lose protections against

remains unsettled is when an individual is a targetable member of such a group. Thus, in the hypothetical vignette, the difficulty is not in deciding whether the U.S. can target the ISIS Commander, but rather whether the brother is also a targetable member of ISIS. Answering this question is important for ensuring State actors, engaged in hostilities with non-State armed groups during a NIAC, are capable of complying with the principle of distinction[7] as well as with their general obligation to protect civilians in the area of hostilities.[8]

There are various legally defensible views on how best to answer this question. Yet, in determining which approach is most reasonable, it is worth noting that the "challenging and complex circumstances of contemporary warfare"[9] require targeting guidance that is easily communicated to the State's armed forces. An approach that is impractical in application will not foster compliance and will create greater risk for the civilian population in these conflicts.

Therefore, in order to strengthen "the implementation of the principle of distinction"[10] in an era of increasingly powerful non-State actors and concomitant violent NIACs,[11] this article seeks to find a targeting approach that is both legal and practical to implement.

The article begins with a background section discussing OAGs, such as ISIS, and the consequences of membership in such a group. A survey of the various methods of determining OAG membership, and the practical applicability of each approach to ISIS, follows. Based upon this comparison, the article concludes that more restrictive membership criteria create an unworkable paradigm that does not match the realities of the modern battlefield. Instead, an expansive understanding

direct attack); *see also* Michael N. Schmitt, *The Status of Opposition Fighters in a Non-International Armed Conflict*, 88 INT'L L. STUD. 119, 137 (2012) ("there is no LOAC prohibition on attacking members of organized armed groups at any time. . . .").

[7] *See* Protocol Additional to the Geneva Conventions of 12 Aug. 1949, and Relating to the Protection of Victims of International Armed Conflict (Protocol I) art. 48, June 8, 1977, 1125 U.N.T.S. 3 [hereinafter AP I] (stating that parties to the conflict must "distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives.").

[8] *See id*. art. 51(2) ("The civilian population as such, as well as individual civilians, shall not be the object of attack."); Protocol Additional to the Geneva Conventions of August 1949, and Relating to the Protection of Victims of Non-International Armed Conflict (Protocol II) art. 13, June 8, 1977, 1125 U.N.T.S. 609 [hereinafter AP II] ("Civilians shall enjoy the protection afforded by this part, unless and for such time as they take a direct part in hostilities.").

While the United States has not ratified AP I or AP II, many portions of the protocol are considered customary international law, including the protection of civilians during conflict and the principle of distinction. *See generally* Michael J. Matheson, *Remarks on the United States Position on the Relation of Customary International Law to the 1977 Protocols Additional to the 1949 Geneva Conventions,* 2 AM. U.J. INT'L L. & POL'Y 419 (1987).

[9] ICRC INTERPRETIVE GUIDANCE, *supra* note 6.

[10] *Id*. at 6.

[11] *See, e.g.*, Shane Reeves, *What Happens When States No Longer Govern*?, LAWFARE (Feb. 13, 2017), https://www.lawfareblog.com/what-happens-when-states-no-longer-govern.

of who qualifies as a member of an OAG is not only practical, but necessary for providing underlying support for the principle of distinction in non-international armed conflicts.

I.
STATUS-BASED TARGETING OF "OTHER" ORGANIZED ARMED GROUPS IN A NON-INTERNATIONAL ARMED CONFLICT

A. What is an "Organized Armed Group" (OAG)?

During a NIAC, Common Article 3 to the 1949 Geneva Conventions[12] is applicable to "each Party to the conflict."[13] Common Article 3 provides no further guidance on party status, only distinguishing between individuals who are taking an "active part in hostilities" and those who are not.[14] Clarification on who qualifies as a "Party to the conflict" in a NIAC is provided by Article 1(1) of the 1977 Additional Protocol II,[15] which states:

[12] There are roughly twelve "common" articles found in the Geneva Conventions. *See* GARY D. SOLIS, THE LAW OF ARMED CONFLICT: INTERNATIONAL HUMANITARIAN LAW IN WAR, 84–85 (2010). Common Article 3, which is repeated verbatim in all four Geneva Conventions, establishes the "law trigger for application of all treaty and customary international law related to" non-international armed conflicts. *See* Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field art. 3, Aug. 12, 1949, 6 U.S.T. 3114, 75 U.N.T.S. 31; Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea art. 3, Aug. 12, 1949, 6 U.S.T. 3217, 75 U.N.T.S. 85 [hereinafter GC I]; Convention Relative to the Treatment of Prisoners of War art. 3, Aug. 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135 [hereinafter GC III]; Convention Relative to the Protection of Civilian Persons in Time of War art. 3, Aug. 12, 1949, 6 U.S.T. 3516, 75 U.N.T.S. 287; *see also* GEOFFREY S. CORN, *Legal Classification of Military Operations*, *in* U.S. MILITARY OPERATIONS: LAW, POLICY, AND PRACTICE 74 (Geoffrey S. Corn, et al. eds. 2016).

[13] *See* GC III, *supra* note 12, art. 3 ("In the case of armed conflict not of an international character occurring in the territory of one of the High Contracting Parties, each Party to the conflict shall be bound to apply, as a minimum, the following provisions . . . .").

[14] *See id*. ("Persons taking no active part in the hostilities, including members of armed forces who have laid down their arms and those placed *hors de combat* by sickness, wounds, detention, or any other cause, shall in all circumstances be treated humanely. . . .").

[15] Again, while the U.S. has not ratified Additional Protocol II many of its provisions are considered customary international law. *See, e.g*., Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, ¶¶ 79, 82 (July 8); Military and Paramilitary Activities in and against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 54, ¶ 218 (June 27); Schmitt, *supra* note 6, at 119 (noting that certain individual provisions of Additional Protocol II are customary); ICRC, *Non-international armed conflict, in* How Does Law Protect in War?, https:// casebook.icrc.org/law/non-international-armed-conflict (last visited Oct. 30, 2017)("The ICRC Study on customary international humanitarian law has confirmed the customary nature of most of the treaty rules applicable in non-international armed conflicts (Art. 3 common to the Conventions and Protocol II in particular).").

> [t]his Protocol, which develops and supplements Article 3 common to the Geneva Conventions of 12 August 1949 without modifying its existing conditions of application, shall apply to all armed conflicts which are not covered by Article 1 of the Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I) and which take place in the territory of a High Contracting Party between its armed forces and dissident armed forces or other organized armed groups which, under responsible command, exercise such control over a part of its territory as to enable them to carry out sustained and concerted military operations and to implement this Protocol.[16]

Thus, Additional Protocol II clearly anticipates non-State groups acting as a party to a NIAC.[17] In particular, the text specifies that, in addition to a State party, other parties to the conflict could include "dissident armed forces" or "other organized armed groups."[18] While it is outside the scope of this article to analyze the "dissident armed forces" language of this provision, it is enough to note this is "the most straightforward category of opposition forces" in a NIAC.[19]

In contrast, "other organized armed groups" only qualify as a "Party to the conflict" if they are "under responsible command" and exercising territorial control such that they can "carry out sustained and concerted military operations."[20] Providing further granularity on what characterizes "sustained and concerted military operations," Article 1(2) makes Additional Protocol II inapplicable to "internal disturbances and tensions, such as riots, isolated and sporadic acts of violence and other acts of a similar nature."[21] Relying on this language, the International Criminal Tribunal for the former Yugoslavia (ICTY) defined a NIAC as "protracted armed violence between governmental authorities and organized armed groups."[22] Assuming the conflict meets the requisite

[16] AP II, *supra* note 8, at art. 1(1).

[17] Additional Protocol II is not as widely applicable as Common Article 3 since it is only triggered if there is involvement of a State armed group (versus a non-international armed conflict exclusively between non-State actors) and the group opposed to the government controls territory. *Compare* GC III, *supra* note 12, art. 3 *with* AP II, *supra* note 8, art 1(1). *See also* YVES SANDOZ ET AL., COMMENTARY ON THE ADDITIONAL PROTOCOLS OF 8 JULY 1977 TO THE GENEVA CONVENTIONS OF 12 AUGUST 1949 ¶ 4447 (1987) [hereinafter COMMENTARY] ("In fact, the Protocol only applies to conflicts of a certain degree of intensity and does not have exactly the same field of application as common Article 3, which applies in all situations of non-international armed conflict."). While these differences "bear on the law that applies to a conflict" it does not alter the status of the participants. Schmitt, *supra* note 6, at 120.

[18] AP II, *supra* note 8, at art. 1(1).

[19] Schmitt, *supra* note 6, at 124. *See id*. 124-26 for an explanation on why "dissident armed forces" are easy to identify. It is also important to note that a civilian that directly participates in the hostilities will forego the protections typically afforded them in in a NIAC. *See* AP II, *supra* note 8, at art. 13.3 (noting that civilians are protected "unless and for such time as they take a direct part in hostilities."). *See also* ICRC INTERPRETIVE GUIDANCE, *supra* note 6 at 25 (describing this category as those "who directly participate in hostilities on a merely spontaneous, sporadic or unorganized basis").

[20] AP II, *supra* note 8, at art. 1(1).

[21] *Id*. at art. 1(2).

[22] Prosecutor v. Tadic, Case No. IT-94-1, Decision on Defence Motion for Interlocutory Appeal on

intensity,[23] the question then becomes under what conditions a collection of fighters can be labeled an "organized armed group" (OAG)?

There appears to be great flexibility in this determination, as the law of armed conflict (LOAC) accepts a broad definition of an OAG.[24] As noted above, Additional Protocol II, Article 1(1) requires the group to be "under responsible command,"[25] a phrase "explicatory of the notion of organization."[26] An OAG, according to the Commentary to the Article, should be an "organization capable, on the one hand, of planning and carrying out sustained and concerted military operations, and on the other, of imposing discipline in the name of a de facto authority." [27] Yet, this does not mean "that there is a hierarchical system of military organization similar to that of regular armed forces."[28] In fact, the International Committee of the Red Cross (ICRC) notes that only minimal organization is necessary.[29]

While there may not be a "rigid, itemized checklist" of criteria that qualifies a group as an OAG,[30] the ICTY does offer helpful factors for making this determination. In the 2005 case of *Limaj*,[31] the ICTY specifically identified the following factors of the Kosovo Liberation Army as persuasive in determining its status as an OAG: the existence of a general staff and headquarters, designated military zones, adoption of internal regulations, the appointment of a spokesperson, coordinated military actions, recruitment activities, the wearing of

Jurisdiction ¶ 70 (Int'I Crim. Trib. for the Former Yugoslavia Oct. 2, 1995). Professor Schmitt notes that the ICTY definition of a NIAC thus "created a test combining intensity and organization which has been adopted in the Rome Statute of the International Criminal Court." Schmitt, *supra* note 6, at 127 (citing Rome Statute of the International Criminal Court art. 8(2)(f), July 17, 1998, 2187 U.N.T.S. 90) (defining a NIAC as taking "place in the territory of a State when there is protracted armed conflict between governmental authorities and organized armed groups or between such groups."). The Tadic definition of a NIAC is generally considered customary international law. *See, e.g.*, International Committee of the Red Cross (ICRC) Opinion Paper, *How is the Term "Armed Conflict" Defined in International Humanitarian Law?* 5 Mar. 2008.

[23] *See* Peter Margulies, *Networks in Non-International Armed Conflicts: Crossing Borders and Defining "Organized Armed Groups*," 89 INT'L L. STUD. 54, 65 (2013) (offering an excellent discussion on how to best interpret the ICTY's use of the term "protracted armed violence.").

[24] *Id*. at 62.

[25] AP II, *supra* note 8, art 1(1).

[26] Schmitt, *supra* note 6, at 128.

[27] COMMENTARY, *supra* note 17, at 1352, ¶ 4463.

[28] *Id*.

[29] *See* INTERNATIONAL COMMITTEE OF THE RED CROSS, HOW IS THE TERM "ARMED CONFLICT" DEFINED IN INTERNATIONAL HUMANITARIAN LAW? 5 Mar. 2008, http://www.icrc.org/eng/assets/files/other/opinion-paper-armed-conflict.pdf (stating "as to the insurgents, the hostilities are meant to be of a collective character, [i.e.,] they have to be carried out not only by single groups. In addition, the insurgents have to exhibit a minimum amount of organisation.").

[30] Margulies, *supra* note 233, at 62.

[31] Prosecutor v. Limaj, Case No. IT-03-66-T, Judgment, 1 90 (Int'I Crim. Trib. for the Former Yugoslavia Nov. 30, 2005) [hereinafter *Limaj*] at 37, ¶ 90.

uniforms and negotiations with the other side.[32] Similarly, in the case of *Haradinaj*,[33] the ICTY again looked at various factors to determine the existence of an organized armed group. These factors included:

> the existence of a headquarters; the fact that the group controls a certain territory; the ability of the group to gain access to weapons, other military equipment, recruits and military training; its ability to plan, coordinate and carry out military operations, including troop movements and logistics; its ability to define a unified military strategy and use military tactics; and its ability to speak with one voice and negotiate and conclude agreements such as cease-fire or peace accords.[34]

An analysis of these two ICTY cases indicate that an OAG, at minimum, should exhibit a degree of structure and be able to act in a coordinated fashion.[35] More specifically, "a group that is transitory or ad hoc in nature does not qualify; in other words, an organized armed group can never simply consist of those who are engaged in hostilities against the State, *sans plus*. It must be a distinct entity that the other side can label the 'enemy'. . . ."[36] However, it is worth highlighting again that the ICTY did not consider any "single factor [as] necessarily determinative" of a group being organized.[37]

A group that is sufficiently "organized" must also be "armed" to qualify as an OAG. "Logically, a group is armed when it has the capacity to carry out 'attacks'"[38] which are defined as "acts of violence against the adversary, whether in offence or in defence."[39] Professor Schmitt notes that "[s]uch acts must be based on the *group's* intentions, not those of individual members. This conclusion derives from the fact that while many members of the armed forces have no violent function, the armed forces as a whole are nevertheless 'armed' as a matter of LOAC."[40] In situations where a group is not directly conducting an attack, but takes action that would be construed as directly participating in hostilities, "it is a reasonable extrapolation to conclude" that the group meets the criteria for being

[32] Schmitt, *supra* note 6, at 129 (citing *Limaj*).

[33] Prosecutor v. Haradinaj, Case No. IT-04-84-T, Judgment, ¶ 60 (Int'l Crim. Trib. for the Former Yugoslavia Apr. 3, 2008), surveying Prosecutor v. Tadic, Case No. IT-94-1-T, Judgment (Int'I Crim. Trib. for the Former Yugoslavia May 7, 1997); *see also* Schmitt, *supra* note 6, at 129.

[34] Prosecutor v. Haradinaj, *supra* note 33, at ¶ 60.

[35] *See* Schmitt, *supra* note 6, at 129–30.

[36] *Id*. at 129.

[37] *Id*. at 129 (citing *Haradinaj*).

[38] *Id*. at 131.

[39] AP I, *supra* note 7, at art. 49(1).

[40] *See* Schmitt, *supra* note 6, at 131. To support this proposition Professor Schmitt draws an analogy to Additional Protocol I Article 43.2 which categorizes "member of the armed forces" as "combatants . . . [who] have the right to participate directly in hostilities," AP I, *supra* note 7, at art. 43.2, "not as individuals who do so participate." Schmitt, *supra* note 6, at n.72. Therefore, it is the group's activities that matter, "not those of select members." *Id*.

"armed."[41] Examples may include those who collect tactical intelligence to be used by another group in carrying out an attack[42] or those who provide weapons for use in an immediate attack.[43] Thus, similar to the term "organized," the definition of "armed" does not appear to be narrowly construed.

Applying the "organized" and "armed" criteria to a contemporary organization is helpful for illustrating the parameters of an OAG. Perhaps no current non-State actor is more relevant to this exercise than ISIS. Therefore, an application of the OAG criteria to ISIS follows.

B. Contemporary Example of an OAG: ISIS

ISIS's ideological and organizational roots are traced to disenfranchised Sunnis who, led by Abu Musab al Zarqawi, grouped together to fight the U.S. and the newly established Iraqi government from 2002-2006.[44] Though Zarqawi was killed by U.S. forces in 2006, the group continued their violent activities, eventually evolving into ISIS.[45] "By early 2013, the group was conducting dozens of deadly attacks a month inside Iraq and had begun operations in neighboring Syria."[46] In June 2014, ISIS declared their intent to re-form a caliphate across large swaths of land in the Middle East, claimed Raqqah, Syria as their capital, and named Abu Bakr al Baghdadi (a former U.S. detainee) as caliph and imam.[47] Heavily armed—as evidenced by their ability to conduct sustained military operations against the U.S. and Coalition partners[48]—ISIS has gone about establishing their caliphate through force, abductions, sexual slavery, beheadings, and public executions.[49] While recent battlefield losses have significantly shrunk

[41] Schmitt, *supra* note 6, at 131 (explaining that "to the extent that acts constituting direct participation render individual civilians subject to attack" it can be concluded that "a group with a purpose of directly participating in hostilities" is also armed).

[42] *See id*.

[43] *See* ICRC INTERPRETIVE GUIDANCE, *supra* note 6, at 55–56 (stating that "[t]he delivery by a civilian truck driver of ammunition to an active firing position at the front line would almost certainly have to be regarded as an integral part of ongoing combat operations and, therefore, as direct participation in hostilities" (citation omitted)).

[44] Blanchard & Humud, *supra* note 1, at 18.

[45] *Id*. *See also* Howard Shatz and Erin-Elizabeth Johnson, *The Islamic State We Knew: Insights Before the Resurgence and Their Implications*, RAND CORPORATION, 5–6 (2015), https://www.rand.org/pubs/research_reports/RR1267.html.

[46] Blanchard & Humud, *supra* note 1, at 18.

[47] *See id*.

[48] *See, e.g*., Tom O'Connor, *War in Iraq: Islamic State Collapses as Military Kills ISIS Commander in West Mosul,* NEWSWEEK (May 10, 2017), http://www.newsweek.com/war-iraq-islamic-state-military-kill-isis-commander-mosul-607055 (discussing a recent combat operation where ISIS used suicide bombers and sniper fire against the U.S. and its coalition partners); Jeremy Wilson, Jeremy Bender & Armin Rosen, *These are the weapons Islamic State fighters are using to terrify the Middle East,* BUSINESS INSIDER (Jan. 17, 2016), http://www.businessinsider.com/isis-military-equipment-arsenal-2016 (discussing heavy weaponry possessed by ISIS including tanks, armored vehicle, self-propelled artillery, rocket launchers, as well as other equipment).

[49] Office of the UN High Comm'r for Human Rights (OHCHR) and UN Assistance Mission for Iraq

the area under ISIS dominance,[50] the group continues to control territory and govern a small group of civilians under a strict version of Sharia law.[51]

The ISIS organizational structure is built around five main pillars: security, sharia, military, administration, and media.[52] Emphasis on each of these pillars allows ISIS to gain, and then maintain, control of territory.[53] In describing the sophisticated organization of ISIS, a RAND study notes that "[t]he group was (and is) bureaucratic and hierarchical. Lower-level units reported to upper-level units, and units shared a basic structure in which upper-level emirs were responsible for security, sharia, military, and administration in a particular geographic area."[54] Further, "[t]hese emirs worked with departments or committees and managed a layer of sector emirs and specialized emirs at lower levels. This structure created a bench of personnel knowledgeable about managing a terrorist group that intended to become a State."[55]

As part of this organizational structure, individuals pledge an oath to ISIS and specifically to its leader, Abu Bakr al Baghdadi.[56] The oath of allegiance,

(UNAMI), Report on the Protection of Civilians in the Armed Conflict in Iraq: 1 May – 31 October 2015, at 8-20 (Jan. 19, 2016), http://reliefweb.int/report/iraq/report-protection-civilians-armed-conflict-iraq-1-may-31-october-2015-enar [hereinafter Report on the Protection of Civilians in the Armed Conflict in Iraq]. See also Shatz & Johnson, *supra* note 455, at 3.

[50] For a map of the areas within Iraq and Syria controlled by ISIS at the time of writing, see Blanchard & Humud, *supra* note 1, at Fig. 1.

[51] *See, e.g.*, *id*. at 26 ("The ideology of the Islamic State organization can be described as a uniquely hardline version of violent jihadist-Salafism—the group and its supporters are willing to use violence in an armed struggle to establish what they view as an ideal society based on their understanding of Sunni Islam."); Shatz & Johnson, *supra* note 45, at 2 ("Clandestine campaigns of assassination and intimidation have been part of the group's playbook for more than a decade.").

[52] *See* Blanchard & Humud, *supra* note 1, at 10.

[53] For example, the RAND report describes the methodical process ISIS follows to gain control of territory:

> establish an intelligence and security apparatus, target key opponents, and establish extortion and other criminal revenue-raising practices; establish administrative and finance functions and lay the foundation for command and control, recruiting, and logistics; establish a sharia network, building relations with local religious leaders; establish a media and information function; [and] establish military cells to conduct attacks.

Shatz & Johnson, *supra* note 45, at 10 (citing Pat Ryan, *AQI in Mosul: Don't Count Them Out*, AL SAHWA (Dec. 15, 2009)).

[54] Shatz & Johnson, *supra* note 45, at 2.

[55] *Id*.

[56] *See* Reem Makhoul & Mark Scheffler, *Pledging Allegiance to ISIS: Real Oath or Empty Symbolism?,* WALL ST. J. (Nov. 13, 2014), http://www.wsj.com/video/pledging-allegiance-to-isis-real-oath-or-empty-symbolism/7B2650B8-A534-4E97-B59F-0BF57BBB7AE9.html; *see also* Blanchard & Humud, *supra* note 1, at 21 ("Since 2014, some armed groups have recognized the Islamic State caliphate and pledged loyalty to Abu Bakr al Baghdadi."), and Priyanka Boghani, *What a Pledge of Allegiance to ISIS Means*, FRONTLINE (Nov. 12, 2014), https://www.pbs.org/wgbh/frontline/article/what-a-pledge-of-allegiance-to-isis-means/ (discussing

called *bay'ah*, is common to the Islamic world. This "[o]ath of allegiance to a leader," is an "[u]nwritten pact given on behalf of the subjects by leading members of the tribe with the understanding that, as long as the leader abides by certain responsibilities towards his subjects, they are to maintain their allegiance to him."[57] In the case of ISIS, when individuals and groups pledge *bay'ah* to the terrorist group, they are pledging an allegiance to the claim by ISIS that it can use any means necessary to reestablish the caliphate and that Abu Bakr al Baghdadi is "the caliph and imam (leader of the world's Muslims)."[58] To dishonor the oath to ISIS and al Baghdadi will result in punishment.[59]

ISIS membership also requires vetting and mentoring from an established member.[60] During this vetting and indoctrination process, aspiring members are required to study selected books, publications, and fatwas provided by ISIS.[61] Upon completion of this initial phase, all potential members must attend Sharia Camp, followed later by military camp.[62] ISIS then assigns its members to various roles, all contributing to the overall mission of the group to establish their caliphate by whatever means necessary. If accepted into ISIS, members are expected to plan, coordinate, and carry out military actions against all those outside of the group including State military forces, State government officials and civilians.[63] As the excerpts from the RAND article evidence, even if an ISIS

various terrorists groups from outside of Iraq and Syria pledging allegiance to ISIS and al-Baghdadi).

[57] Oxford Islamic Studies Online, Oxford University Press, at http://www.oxfordislamicstudies.com/article/ opr/t125/e316.

[58] Blanchard & Humud, *supra* note 1, at 18 ("In June 2014, Islamic State leaders declared their reestablishment of the caliphate . . . demanded the support of believing Muslims, and named Abu Bakr al Baghdadi as caliph and imam . . . ."). *See also* Thomas Joscelyn & Caleb Weiss, *Islamic State recognizes oath of allegiance from jihadists in Mali*, FDD'S LONG WAR JOURNAL (Oct. 31, 2016), https://www.longwarjournal.org/archives/2016/10/islamic-state-recognizes-oath-of-allegiance-from-jihadists-in-west-africa.php.

[59] Makhoul & Scheffler, *supra* note 566 ("Breaking a pledge is a considered a great sin and even if ISIS doesn't punish you, God will.").

[60] *See generally* Wissam Abdallah, *What it takes to join the Islamic State*, AL-MONITOR (Aug. 6, 2015), http://www.al-monitor.com/pulse/politics/2015/08/syria-fighters-join-isis-apply-training-requirements.html (articulating the intense, detailed and long process for joining ISIS including military training for *all* members of ISIS, even those who do not ultimately conduct direct attacks); John Graham, *Who Joins ISIS and Why?*, HUFFINGTON POST BLOG, http://www.huffingtonpost.com/john-graham/who-joins-isis-and-why_b_8881810.html (addressing the "great lengths" that ISIS has gone to "to demonstrate to its members and recruits that the world of radical Islam is not just death and destruction but a 24/7 total support structure" as part of the continuing indoctrination of ISIS members); Alessandria Masi, *ISIS Recruiting Westerners: How the "Islamic State" Goes After Non-Muslims and Recent Converts in the West*, IB TIMES (Sept. 8, 2014), http://www.ibtimes.com/isis-recruiting-westerners-how-islamic-state-goes-after-non-muslims-recent-converts-west-1680076 (describing how ISIS requires the establishment of an in-depth mentor-recruit relationship as part of the vetting process for Westerners who want to join ISIS).

[61] *See* Abdallah, *supra* note 600.

[62] *Id*.

[63] *See generally* Blanchard & Humud, *supra* note 1, at 21–25 (describing the various ISIS attacks around the world). *See also* Report on the Protection of Civilians in the Armed Conflict in Iraq, *supra* note 49.

member operates in a seemingly non-military role, their actions contribute to the overall violent and combative nature of the organization which, again, has the ultimate goal to take over territory through any means.

Based on the above information, ISIS is a hierarchical organization that is well-armed and qualifies as an OAG. Further, the group is currently participating in a number of NIACs[64] and is thus a "Party to the conflict." Accordingly, membership in ISIS, if established, results in the adverse consequences described below.

C. Consequence of Being a Member of an OAG

In a NIAC an individual may be a civilian, part of the government's armed forces,[65] or a member of an OAG.[66] These are mutually exclusive categories, meaning members of an OAG are obviously not civilians.[67] This distinction is not unimportant as the protections extended to civilians by the LOAC will not apply to OAG members.[68] In particular, whereas civilians are only targetable "for such time as they take a direct part in hostilities,"[69] OAG members are "analogous to members of the armed forces, and thereby remain targetable even when not participating" in the hostilities.[70] In other words, a civilian's *conduct* determines

---

[64] *See generally* David Wallace, Amy McCarthy & Shane R. Reeves, *Trying to Make Sense of the Senseless: Classifying the Syrian War under the Law of Armed Conflict,* 25 MICH. ST. INT'L L. REV. 555 (2017).

[65] *See generally* Sean Watts, *Present and Future Conceptions of the Status of Government Forces in Non-International Armed Conflict*, 88 INT'L L. STUD. 145 (2012) (discussing this particular battlefield status).

[66] *See* DOD LAW OF WAR MANUAL, *supra* note 6, at ¶ 5.9.2.1 (citing Stephen Pomper, *Toward a Limited Consensus on the Loss of Civilian Immunity in Non-International Armed Conflict: Making Progress Through Practice*, 88 INT'L L. STUD. 188, 193 n.22 (2012)).

> The U.S. approach has generally been to refrain from classifying those belonging to non-State armed groups as "civilians" to whom this rule would apply. The U.S. approach has been to treat the status of belonging to a hostile, non-State armed group as a separate basis upon which a person is liable to attack, apart from whether he or she has taken a direct part in hostilities.

Id. For a detailed discussion on whether "organized armed groups other than the dissident armed forces comprise groups who are directly participating in hostilities or constitute a separate category of 'non-civilians,'" see also ICRC INTERPRETIVE GUIDANCE, *supra* note 6, at 28; Schmitt, *supra* note 6, at 127.

[67] *See, e.g.*, DOD LAW OF WAR MANUAL, *supra* note 6, at ¶ 5.9.2.1.

[68] *See* Schmitt, *supra* note 6, at 128 ("for if members of an organized armed group are not civilians, the LOAC extending protection to civilians is inapplicable to them.").

[69] AP II, *supra* note 8, at art. 13(3).

[70] Schmitt, *supra* note 6, at 127. *See* DOD LAW OF WAR MANUAL, *supra* note 6, at ¶ 5.8.3 ("Like members of an enemy State's armed forces, individuals who are formally or functionally part of a non-State armed group that is engaged in hostilities may be made the object of attack because they likewise share in their group's hostile intent."); REPORT ON THE LEGAL AND POLICY FRAMEWORKS GUIDING THE UNITED STATES' USE OF MILITARY FORCE AND RELATED NATIONAL SECURITY OPERATIONS 20

whether they are targetable, whereas a member of an OAG is targetable "at any time during the period of their membership,"[71] and thus is vulnerable to attack due to their status as a member of the group.[72]

Additionally, as there is no prisoner of war regime or concept of "combatant immunity" in a NIAC,[73] an OAG member upon capture "may be put on trial for treason or other crimes, and heavily punished."[74] These prosecutions are not restricted to only violations of the LOAC or war crimes, but also "for any acts that violate domestic law" including "attacking members of the armed forces."[75] Of course basic rights, such as due process and protection from summary execution, apply to these proceedings,[76] as an OAG member is treated as any other domestic criminal for their participation in the NIAC.

(Dec. 2016) [hereinafter REPORT ON THE LEGAL AND POLICY FRAMEWORKS GUIDING THE UNITED STATES' USE OF MILITARY FORCE] (discussing the U.S. approach to targeting individuals in a NIAC).

[71] Schmitt, *supra* note 6, at 132.

[72] *See, e.g.*, DOD LAW OF WAR MANUAL, *supra* note 6, at ¶ 5.7.1 stating:

> Membership in the armed forces or belonging to an armed group makes a person liable to being made the object of attack regardless of whether he or she is taking a direct part in hostilities . . . . This is because the *organization's hostile intent may be imputed to an individual through his or her association with the organization*. Moreover, the individual, as an agent of the group, can be assigned a combat role at any time, even if the individual normally performs other functions for the group. Thus, combatants may be made the object of attack at all times, regardless of the activities in which they are engaged at the time of attack. For example, combatants who are standing in a mess line, engaging in recreational activities, or sleeping remain the lawful object of attack, provided they are not placed *hors de combat*.

See also Rachel E. VanLandingham, *Meaningful Membership: Making War a Bit More Criminal*, 35 CARDOZO L. REV. 79, 105 (2013) ("[B]ecause the belligerent is presumptively hostile at all times, this allows the direct attack of fighters, *once properly identified as such*, at any time during an armed conflict, whether or not they are doing anything related to hostilities at the time. . . .").

[73] *See, e.g.*, UNITED KINGDOM MINISTRY OF DEFENCE, THE JOINT SERVICE MANUAL OF THE LAW OF ARMED CONFLICT ¶ 15.6.1 (2004) [hereinafter UK MANUAL] ("The law relating to internal armed conflict does not deal specifically with combatant status. . . ."); DOD LAW OF WAR MANUAL, *supra* note 6, at ¶ 17.4.1.1 (discussing how members of a non-State armed group are not afforded combatant immunity).

[74] Michael N. Schmitt, Charles H.B. Garraway, & Yoram Dinstein, THE MANUAL ON THE LAW OF NON-INTERNATIONAL ARMED CONFLICT WITH COMMENTARY 41 (International Institute of Humanitarian Law, 2006) [hereinafter NIAC MANUAL] (noting "[i]t should be understood, however, that trial and punishment must be based on due process of law").

[75] *See, e.g.*, DOD LAW OF WAR MANUAL, *supra* note 6, at ¶ 17.4.1.1 (discussing a State's power to prosecute non-State actors in a NIAC for their actions under domestic law); UK MANUAL, *supra* note 73, at ¶ 15.6.3 (stating "[a] captured member of dissident fighting forces is not legally entitled to prisoner of war status"); *see also* Schmitt, *supra* note 6, at 121("[T]here is no prisoner of war regime in the context of a non-international armed conflict.").

[76] *See* UK MANUAL, *supra* note 733, at ¶ 15.6.4 ("Nevertheless, the law of non-international armed conflict clearly requires that any person . . . detained by either dissident or government forces must be treated humanely"); NIAC MANUAL, *supra* note 744, at 41; *see also* GC III, *supra* note 122, at art. 3.

The consequences of being a member of ISIS, particularly exposure to status-based targeting and prosecution for engaging in combat operations, are significant. But what makes an individual a targetable member of ISIS? For example, is swearing an oath of loyalty to al Baghdadi, being listed on an authenticated ISIS membership roster, or enforcing the group's strict form of sharia law in captured territory evidence enough for status-based targeting?[77] More broadly, what qualifies an individual as a member of an OAG versus simply being affiliated with such a group? There are a number of proposed answers to this question which are discussed in the following section.

II.
SURVEYING THE FIELD: APPROACHES TO DETERMINING MEMBERSHIP IN AN OAG

Again, membership in an OAG makes an individual vulnerable to the consequences associated with such a status.[78] The LOAC provides minimal guidance on who qualifies as a member of an OAG,[79] leaving much discretion to States' armed forces when making these decisions.[80] In an effort to address this ambiguity, and to clarify the line separating civilian and conflict participant, various approaches to determining OAG membership have emerged.

A. Continuous Combat Function (CCF)

The ICRC's *Interpretive Guidance* offers a narrow interpretation of who qualifies as a member of an OAG. The *Guidance* provides that a non-State party involved in a NIAC, similar to the State party, may have a component that is separate and distinct from the armed faction "such as political and humanitarian wings."[81] Only those acting as the fighting forces or armed wing of the non-State party are potentially considered members of the OAG and therefore non-civilians.[82] Furthermore, there "may be various degrees of affiliation with [the non-State] group that do not necessarily amount to 'membership' within the

[77] *See generally* Report on the Protection of Civilians in the Armed Conflict in Iraq, *supra* note 49, at 5-20.

[78] *See, e.g.*, DOD LAW OF WAR MANUAL, *supra* note 6, at ¶ 17.4.1.1; ICRC INTERPRETIVE GUIDANCE, *supra* note 6, at 22 (explaining why individual members of an OAG should not be considered civilians); Schmitt, *supra* note 6, at 127-28 (supporting the Interpretive Guidance's distinction between civilians and members of an OAG).

[79] *See* COMMENTARY, *supra* note 177, at 512 ¶ 1672 ("The term 'organized' . . . should be interpreted in the sense that the fighting should have a collective character, be conducted under proper control and according to rules, as opposed to individuals operating in isolation with no corresponding preparation or training.").

[80] *See* VanLandingham, *supra* note 72, at 117.

[81] ICRC INTERPRETIVE GUIDANCE, *supra* note 6, at 32.

[82] *Id.*

meaning of [International Humanitarian Law] IHL."[83] Affiliation may turn on "individual choice . . . involuntary recruitment . . . [or] on more traditional notions of clan or family."[84] Thus, according to the *Guidance,* there are a number of individuals affiliated in some capacity with the non-State party that are not members of the OAG.[85]

To help make this nuanced distinction, the *Guidance* notes that the "decisive criteria . . . is whether a person assumes a continuous function for the group involving his or her direct participation in hostilities."[86] More specifically, an individual must demonstrate a "continuous combat function" (CCF) to qualify as a member of an OAG.[87] In outlining the parameters of the concept the *Guidance* states: "[c]ontinuous combat function requires lasting integration into an organized armed group acting as the armed forces of a non-State party to an armed conflict."[88]

"Lasting integration" through a CCF does not include those "persons comparable to reservists who, after a period of basic training or active membership, leave the armed group and re-integrate into civilian life."[89] Additionally, those who "continuously accompany or support an organized armed group, but whose function does not involve direct participation in hostilities" are

---

[83] *Id*. at 33.

[84] *Id*.

[85] *Id*. at 34 (stating "[i]ndividuals who continuously accompany or support an organized armed group, but whose function does not involve direct participation in hostilities, are not members of that group within the meaning of IHL").

[86] *Id*. What qualifies as "direct participation in hostilities" is debatable and outside the scope of this article. *Compare* ICRC INTERPRETIVE GUIDANCE, *supra* note 6, at 5-6 ("The Interpretive Guidance provides a legal reading of the notion of 'direct participation in hostilities' with a view to strengthening the implementation of the principle distinction.") *with* Kenneth Watkin, *Opportunity Lost: Organized Armed Groups and the ICRC 'Direct Participation in Hostilities' Interpretive Guidance*, 42 N.Y.U. J. INT'L L. & POL. 641, 646 (No. 3, 2010) *and* Michael N. Schmitt, *The Interpretive Guidance on the Notion of Direct Participation in Hostilities: A Critical Analysis*, 1 HARV. NAT. SEC. J. 1, 5 (May 2010) (criticizing the Interpretive Guidance legal reading of the term).

[87] *See* Schmitt, *supra* note 6, at 132 ("[B]y the *Guidance* standard only those with a continuous combat function may be treated as members of an organized armed group and therefore attackable at any time during the period of their membership.").

[88] ICRC INTERPRETIVE GUIDANCE, *supra* note 6, at 34. Further clarifying what qualifies as a CCF, the *Guidance* states:

> Individuals whose continuous function involves the preparation, execution, or command of acts or operations amounting to direct participation in hostilities are assuming a continuous combat function. An individual recruited, trained and equipped by such a group to continuously and directly participate in hostilities on its behalf can be considered to assume a continuous combat function even before he or she first carries out a hostile act.

Id.

[89] *Id*.

also not in a CCF.[90] These individuals, while clearly contributing to the OAG's efforts, are considered civilians.[91] "As civilians, they benefit from protection against direct attack unless and for such time as they directly participate in hostilities, even though their activities or location may increase their exposure to incidental death or injury."[92]

B. Conduct-Link-Intent Test

Finding the ICRC's *Interpretive Guidance* test too restrictive, but recognizing that "today's enemy groups lack obvious indicia of targetable membership, and the LOAC provides no methodology for its ascertainment,"[93] Professor VanLandingham offers an alternative analysis. Making an analogy to criminal law statutes, Professor VanLandingham develops three criteria that an individual must satisfy to qualify for OAG membership.[94] First, the conduct exhibited by the individual must fall within an express listing of categories of eligible conduct.[95] This categorization would "help standardize and clarify the identification process, using behavior that has been shown to indicate membership as an analytical start point."[96] The list of conduct, akin to that provided in a U.S. criminal statute, would "force decision-makers to use a defendable, objective template."[97]

---

[90] *Id*.

[91] *Id*. More specifically, according to the *Guidance,* these individuals:

> remain civilians assuming support functions, similar to private contractors and civilian employees accompanying State armed forces. Thus, recruiters, trainers, financiers and propagandists may continuously contribute to the general war effort of a non-State party, but they are not members of an organized armed group belonging to that party unless their function additionally includes activities amounting to direct participation in hostilities. The same applies to individuals whose function is limited to the purchasing, smuggling, manufacturing and maintaining of weapons and other equipment outside specific military operations or to the collection of intelligence other than of a tactical nature. Although such persons may accompany organized armed groups and provide substantial support to a party to the conflict, they do not assume continuous combat function and, for the purposes of the principle of distinction, cannot be regarded as members of an organized armed group.

Id.

[92] ICRC INTERPRETIVE GUIDANCE, *supra* note 6, at 35.

[93] VanLandingham, *supra* note 72, at 137.

[94] *Id*. at 125–28.

[95] *See id*. at 136 ("For example, staying in a known Al-Qaeda guesthouse has been viewed as conduct that indicates Al-Qaeda membership").

[96] *Id*. at 137.

[97] *Id*.

Second, an express associative link between the individual's conduct and the OAG is required.[98] While requiring identification of the conduct-associate link may seem inherent in the eligible conduct list, "carving it out as an express element ensures that purely independent action is not mistakenly included."[99] Further, an associative link "challenges assumptions that may be present in the type of conduct being analyzed"[100] by requiring decision-makers to explain why the activity has been so labeled. Third, the individual must have the specific intent to further the group's violent ends via group orders, which can be inferred from particular types of conduct.[101] Therefore, it is not enough to passively support the OAG, but rather, there must be a willingness to carry out the group's commands.[102]

Application of this conduct-link-intent test would most likely increase the number of individuals considered members of an OAG and, consequently, broaden the population exposed to the consequences of such membership. However, an elements-based analysis of OAG membership that resembles a criminal statute reduces flexibility in making these determinations, particularly for commanders making real-time targeting decisions. Another approach for determining OAG membership, discussed next, is to "treat all armed forces the same."[103]

C. Structural Membership

As both States and non-State actors execute warfare through "the exercise of command, planning, intelligence, and even logistics functions," a structural membership approach argues that there is no reason to distinguish between a State's regular armed forces and "irregular" armed forces.[104] In fact, OAGs

---

[98] *See id*. ("For example, the associative link in staying in an Al-Qaeda guesthouse is the assessment that it is indeed such a guesthouse").

[99] *Id*. at 137.

[100] *Id*.

[101] *See id*. at 137-38. This criteria therefore

> requires an inquiry into why the individual acted the way he did; for example, why the individual planted an IED, provided transportation, or provided lodging. Was he paid to do so, and therefore the answer is for financial gain to feed his family? Or did he do so out of the desire to see the group achieves its objectives via violent means and because he was asked or told to do so by others in the group.

Id. at 138.

[102] *Id*. (noting that those unwilling to carry out the OAG's command do "not symbolically represent the group.").

[103] *See generally* Watkin, *supra* note 866, at 690. Brigadier General Watkin retired as the Judge Advocate General of the Canadian Forces in 2010 and wrote his article in response to the ICRC's Interpretive Guidance.

[104] *Id*.

typically "have a membership structure based on more than mere function"[105] as "it is [the] organization which fights as a group."[106] Therefore, "individuals are simply members of armed forces regardless of which party to a conflict they fight for, the domestic law basis of their enrollment, or whether they wear a uniform."[107] All that is necessary for the consequences of OAG membership to attach to an individual is whether they are "a member of an organization under a command structure."[108]

Of course, not all individuals sympathetic or affiliated with the group are subject to status-based targeting.[109] One who generically creates propaganda or broadly finances the OAG, without more, is not under command or filling a traditional military role.[110] The assumption is, therefore, they are not part of the OAG and are civilians. Again, the key factor "in determining if a person can be attacked is whether the individual is a member of the armed forces . . . under a command responsible for the conduct of its subordinates."[111] It is also important to note, from an operational perspective, the Rules of Engagement (ROE) establish left and right parameters on who is within the OAG.[112]

There may also be individuals, in the command structure, not subject to the adverse consequences of their membership. For example, those who are exclusively in the role of a spiritual leader or doctor would be comparable to

[105] Schmitt, *supra* note 6, at 132.

[106] Watkin, *supra* note 866, at 691.

[107] *Id*. at 690–691.

[108] *Id*. at 691.

[109] For example, the Israeli Defense Force (IDF) agrees that members of an OAG are subject to status-based targeting and also recognizes that there may be military and non-military wings of a non-State actor. *See* Michael N. Schmitt & John J. Merriam, *The Tyranny of Context: Israeli Targeting Practices in Legal Perspective*, 37 U. PA. J. INT'L L. 55, 113 (2017). Those who are part of the non-military branch are subject to targeting if they directly participate in hostilities. *See id*. at 113–14. To help clarify what "direct participation in hostilities" includes the IDF maintains a list of activities that meet this definition. *See id*. Of course it is "impossible for the list to contain all possible forms of direct participation. . . . Therefore, if a commander of an Attack Cell believes an individual is directly participating but the activity concerned does not appear on the list, the commander may elevate the matter to higher authorities for authorization to strike." *Id*.

[110] *See id*. at 107 (discussing why the IDF has taken the position that having a role in generating propaganda or promoting morale does not deprive an individual of civilian status).

[111] *See* Watkin, *supra* note 866, at 691.

[112]Rules of engagement are defined as "[d]irectives issued by competent military authority that delineate the circumstances and limitations under which United States forces will initiate and/or continue combat engagement with other forces encountered." JOINT CHIEFS OF STAFF, JOINT PUB'N 1-02, DEP'T OF DEF. DICTIONARY OF MILITARY AND ASSOCIATED TERMS 472 (2001). In particular, the ROE "establish fundamental policies and procedures governing the actions to be taken by US commanders" during a military operation. JOINT CHIEFS OF STAFF, INSTR. 3121.01B, THE STANDING RULES OF ENGAGEMENT/STANDING RULES FOR THE USE OF FORCE FOR U.S. FORCES app. A, at 95 (2005). Combining operational requirements, policy, and international law therefore make the ROE more restrictive than the law of armed conflict. Supplemental measures, which "enable commanders to tailor ROE for specific missions," are the recognized tool to implement restrictions on the use of force for particular "political and military goals that are often unique to the situation." *Id*. app. A, at 99.

chaplains or medical personnel in a State's armed forces and therefore not targetable.[113] Finally, protections extend to those civilians who "provide services such as selling food under contract or otherwise much like civilian contractors working with regular State armed forces" unless "and for such time as they participate directly in hostilities."[114]

Focusing on the membership structure is therefore like other targeting principles in that it provides a definitional framework allowing for command discretion. For example, Additional Protocol I, Article 52(2), in regards to targeting military objectives, States "[a]ttacks shall be limited strictly to military objectives."[115] The protocol goes on to give broad contours of what is considered a military objective without attempting to provide specific examples.[116] Similarly, under this approach, OAG membership, like an individual's status in a regular State armed force, is possible to confirm in a number of ways. Indicia of membership would include "carrying out a combat function" such as being involved in "combat, combat support, and combat service support functions, carrying arms openly, exercising command over the armed group, [or] carrying out planning related to the conduct of hostilities."[117] However, "the combat function is not a definitive determinant of whether a person is a member of an armed group, but rather one of a number of factors that can be taken into consideration."[118]

The *Department of Defense Law of War Manual* provides guidance for U.S. forces to determine membership by offering non-exhaustive lists of both "formal" and "informal" indicators. Formal indicators, also called "direct information" include: "rank, title, style of communication; taking an oath of loyalty to the group or the group's leader; wearing a uniform or other clothing, adornments, or body markings that identify members of the group; or documents

---

[113] *See* GC I, *supra* note 12, at art. 24.

> Medical personnel exclusively engaged in the search for, or the collection, transport or treatment of the wounded and sick, or in the prevention of disease, staff exclusively engaged in the administration of medical units and establishments, as well as chaplains attached to the armed forces, shall be respected and protected in all circumstances.

Id. While Article 24 is only applicable in an IAC it is valuable for this discussion as it helps establish the status parameters of OAG members.

[114] Watkin, *supra* note 86, at 692.

[115] AP I, *supra* note 7, at art. 52(2).

[116] *See id*. ("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.").

[117] Watkin, *supra* note 86, at 691.

[118] *Id*.

issued or belonging to the group that identify the person as a member… ."[119] Informal factors that help determine OAG membership include:

> acting at the direction of the group or within its command structure; performing a function for the group that is analogous to a function normally performed by a member of a State's armed forces; taking a direct part in hostilities, including consideration of the frequency, intensity, and duration of such participation; accessing facilities, such as safehouses, training camps, or bases used by the group that outsiders would not be permitted to access; traveling along specific clandestine routes used by those groups; or traveling with members of the group in remote locations or while the group conducts operations.[120]

Membership, therefore, includes more than just those engaging in an attack or carrying out a combat function.[121] Rather, what is important is whether the individual is "carrying out substantial and continual integrated support functions."[122] Or, to put it more simply, an individual who is under command, acting in a traditional military role, is subject to the adverse consequences of being an OAG member—in particular, status-based targeting.[123] Recognizing a member of an OAG is often not difficult as these groups consistently distinguish

[119] DOD LAW OF WAR MANUAL, *supra* note 6, at ¶ 5.7.3.1. The first set of factors focus on documents illustrating membership, while the second set focuses on direct observation of certain activities that may indicate membership. The Manual makes clear that these lists provide illustrative examples and are not exhaustive.

[120] *Id*.

[121] *See, e.g.*, DOD LAW OF WAR MANUAL, *supra* note 6, at ¶ 5.7.3 ("individuals who are formally or functionally part of a non-State armed group" are subject to attack); REPORT ON THE LEGAL AND POLICY FRAMEWORKS GUIDING THE UNITED STATES' USE OF MILITARY FORCE, *supra* note 700, at 20. *See also* Watkin, *supra* note 86, at 691–92 ("Someone who provides logistics support as a member of an organized armed group, including cooks and administrative personnel, can be targeted in the same manner as if that person was a member of regular State armed forces.")

[122] *Id*. at 644.

[123] *See, e.g.*, DOD LAW OF WAR MANUAL, *supra* note 6, at ¶ 5.8.3; REPORT ON THE LEGAL AND POLICY FRAMEWORKS GUIDING THE UNITED STATES' USE OF MILITARY FORCE, *supra* note 700, at 29.

> To determine whether an individual is "part of" an enemy force, the United States may rely on either a formal or function analysis of the individual's role in that enemy force (citation omitted). . . . [S]uch a functional analysis may include looking to, among other things, the extent to which that person performs functions for the benefit of the group that are analogous to those traditionally performed by members of a country's armed forces; whether that person is carrying out or giving orders to others within the group; and whether that person has undertaken certain acts that reliably connote meaningful integration into the group.

Id. ISIS members, for example, who recruit or are involved in logistics are comparable to military recruiters and logisticians and would therefore be considered targetable by the United States. *See* DOD LAW OF WAR MANUAL, *supra* note 6, at ¶ 5.8.3 ("Like members of an enemy State's armed forces, individuals who are formally or functionally part of a non-State armed group that is engaged in hostilities may be made the object of attack because they likewise share in their group's hostile intent (citation omitted).")

themselves from the civilian population.[124] However, in more difficult situations, intelligence may confirm membership.[125] Confirmation methods may include human sources, communications intercepts, captured documents, interrogations, as well as a myriad of other available tools.[126] If it is not possible to make such a determination than that person "shall be considered to be a civilian" and afforded the appropriate protections.[127]

III.
WHAT OAG MEMBERSHIP DETERMINATION APPROACH BEST WORKS ON THE CONTEMPORARY NIAC BATTLEFIELD

This section is not intended to re-hash the debates that immediately followed the 2009 release of the ICRC's *Interpretive Guidance*.[128] Instead, the following analysis is offered to illustrate which of the above described approaches best addresses the realities of a contemporary NIAC. In doing so, the hope is to provide clarity as to where the line lies between a civilian and a member of an OAG, therefore decreasing mistakes as to an individual's battlefield status. Again, applying facts from the current conflicts involving ISIS is illustrative.

---

[124] *See generally* Simon Tomlinson, *From the 'Afghani robe' to the suicide bomber's all-black uniform, how ISIS differentiates between ranks and various outfits*, DAILYMAIL.COM (Sept. 29, 2015, 10:14 AM), http://www.dailymail.co.uk/news/article-3253113/From-Afghani-robe-suicide-bomber-s-black-uniform-ISIS-differentiates-ranks-various-outfits.html (explaining how ISIS has corresponding uniforms for each of its units and describing the various outfits). These groups are often in a command structure, have a "fixed distinctive sign recognizable at a distance," and carry their arms openly. In an international armed conflict these are all indications of a militia which, if belonging to a Party to the conflict, have met three of the four criteria to be considered combatants. *See* GC III, *supra* note 12, at art. 4(A)(2). However, rarely, if ever, do these groups comply with the four criteria which is to "conduct their operations in accordance with the laws and customs of war." *Id*. Regardless, these groups show many characteristics of a State's regular armed forces. *See* Schmitt, *supra* note 6, at 132 ("For example, the Red Army, Hamas, Hezbollah, FARC, Tamil Tigers and Kosovo Liberation Army were often distinguishable from the civilian population and operated in a manner not unlike the regular armed forces.")

[125] *See, e.g.*, DOD LAW OF WAR MANUAL, *supra* note 6, at ¶ 5.8.3–4; REPORT ON THE LEGAL AND POLICY FRAMEWORKS GUIDING THE UNITED STATES' USE OF MILITARY FORCE, *supra* note 70, at 20; Watkin, *supra* note 86, at 692.

[126] *See, e.g.*, REPORT ON THE LEGAL AND POLICY FRAMEWORKS GUIDING THE UNITED STATES' USE OF MILITARY FORCE, *supra* note 700, at 20 ("the United States considers all available information about a potential target's current and historical activities to inform an assessment of whether the individual is a lawful target"); Schmitt, *supra* note 6, at 132.

[127] AP I, *supra* note 7, at art. 50(1). The rule is generally considered customary in both an IAC and NIAC. *See* Schmitt, *supra* note 6, at 133 (*citing* 1 CUSTOMARY INTERNATIONAL HUMANITARIAN LAW 23-24 (Jean-Marie Henckaerts & Louise Doswald-Beck eds., 2005.)) However, the United States rejects the Additional Protocol definition of "combatant" as it is viewed as relaxing "the requirements for obtaining the privilege of combatant status" thus undercutting the principle of distinction. DOD LAW OF WAR MANUAL, *supra* note 6, at ¶ 4.6.1.2, 4.8.1.4.

[128] *See generally* Ryan Goodman & Derek Jinks, *The ICRC Interpretive Guidance on the Notion of Direct Participation in Hostilities Under International Humanitarian Law: An Introduction to the Forum,* 42 N.Y.U. J. INT'L L. & POL. 637, 637–640 (2010) (introducing a number of articles written by prominent LOAC and military experts that are critical of the *Interpretive Guidance*).

A. The CCF and the Danger of Good Intentions

The CCF criteria, which sets "a high bar for membership," appears "to afford the civilian population enhanced protection from mistaken attacks" by narrowly interpreting who is an OAG member.[129] This restrictive interpretation would thus seem to result in additional protections for civilians by severely limiting those who have met membership criteria. However, in fact, the CCF approach potentially puts civilians at greater risk. By contrasting those who serve in combat functions against others closely aligned with the OAG, the CCF criteria creates a category of "members of an organized armed group who do not directly participate in hostilities."[130] These individuals, in effect, "allow the entire civilian population to become conflated with the enemy, and exposes all civilians to greater risk."[131]

A short discussion on the evolution of the definition of "protracted armed violence" illustrates the danger of a narrow view on who qualifies as an OAG member. In the *Haradinaj* case the ICTY found that "protracted armed violence," as used in *Tadić*, was "interpreted in practice… as referring more to the intensity of the armed violence than to its duration."[132] This interpretation supported an earlier finding that the brief duration of an attack did not preclude a conflict from being characterized as non-international.[133] Professor Peter Margulies notes that the ICTY referring "generally to the intensity of the violence, not its timing per se" was a pragmatic decision to avoid creating perverse incentives.[134] Otherwise, if "violent non-State actors could strike first and then claim that the conflict was not yet a protracted one" States would be precluded "from utilizing the full range of responses permissible under LOAC" limited instead "to the far narrower repertoire of force permissible under a law enforcement paradigm."[135] Thus, to avoid encouraging this bad behavior, the ICTY adopted a broad interpretation of "protracted armed violence."

---

[129] *See* Schmitt, *supra* note 6, at 132.

[130] VanLandingham, *supra* note 722, at 126.

> In other words, the ICRC's position is that instead of analogizing to the entire composition of a state's military, which includes members who rarely, if ever, fire weapons (such as legal advisors and public affairs officers), its 'continuous combat function' test for belligerent membership in a non-state armed group focuses exclusively on those who engage in either actual combat or in sufficiently hostile activity.

Id.

[131] *Id*. at 131–32.

[132] *See* Prosecutor v. Haradinaj, *supra* note 33, at ¶ 49.

[133] *See* Abella v. Argentina, Case 11.137, Inter-Am. Comm'n H.R.,Report No. 55/97, ¶ 152 (1997).

[134] Margulies, *supra* note 23, at 65.

[135] *Id*.

Similarly, a narrow notion of what makes an individual a targetable member of an OAG creates perverse incentives. By granting "protected civilian status to persons who are an integral part of the combat effectiveness of an OAG,"[136] individuals are encouraged to straddle the line between civilian and non-civilian. What is the status of an ISIS fighter who transitions for a period of time into a cook?[137] It is unclear when this individual ceases their combat function and assumes their non-combat function. Of course, if only members of an OAG who perform a CCF are targeted, much of this confusion may disappear. However, this restrictive approach ignores the organizational aspect of an OAG and the inherent agency relationship of these groups with their members.[138]

For example, the nature of ISIS is that the entire organization is a non-State "organized" and "armed" group.[139] While individuals may join ISIS for any number of reasons,[140] when joining a group whose objectives are to use any level of violence to effectuate their vision, those individuals demonstrate intent to use violent means to assist the group in meeting its objectives.[141] ISIS membership thus evidences what VanLandingham defines as an "inherent agency relationship of command [that] demonstrates a submission of self to the central, overarching, violent purpose of the group."[142] In other words, even those ISIS members not directly involved in combat remain part of the OAG.[143] Requiring an application of the CCF criteria to every individual ISIS member thus ignores the reality that these individuals are fighting under the command structure of a cohesive group.

Finally, the CCF approach creates an inequity between ISIS members and the State's armed forces by providing protections for the former that are not available to the latter.[144] Professor Schmitt notes that, in application, a direct attack

---

[136] Watkin, *supra* note 86, at 675.

[137] For a similar example, see generally *id*. at 676.

[138] *See, e.g*., DOD LAW OF WAR MANUAL, *supra* note 6, at ¶ 5.8.1 ("the individual, as an agent of the group, can be assigned a combat role at any time, even if the individual normally performs other functions for the group."); Gherbi v. Obama, 609 F. Supp. 2d 43, 69 (D.D.C.) (stating "many members of the armed forces who, under different circumstances, would be 'fighters' may be assigned to non-combat roles at the time of their apprehension" and that "[t]hese individuals are no less a part of the military command structure of the enemy, and may assume (or resume) a combat role at any time because of their integration into that structure."). *See also* VanLandingham, *supra* note 72, at 126. Again, ISIS is a helpful example as that group ensures all members receive military training as they are all expected to be fighters. *See supra* text accompanying notes 60–64.

[139] *See supra* text accompanying notes 44–64.

[140] *See* Patrick Tucker, *Why Join ISIS? How Fighters Respond When You Ask Them: A Study Finds that Motivations Vary Widely*, THE ATLANTIC (Dec. 9, 2015), https://www.theatlantic.com/international /archive/2015/12/why-people-join-isis/419685/ (discussing a study conducted on a non-random sample of ISIS fighters that found that some members join ISIS for status, some for identity or revenge, and some for the thrill of it, among other motivations).

[141] VanLandingham, *supra* note 72, at 108.

[142] *Id*.

[143] *See, e.g*., *supra* text accompanying notes 44–64.

[144] *See* Watkin, *supra* note 866, at 693 ("The Interpretive Guidance also adopts a position which clearly disadvantages States in relation to organized armed groups against which they are engaged in armed

on a member "of an organized armed group without a continuous combat function is prohibited (indeed, such an attack would be a war crime since the individual qualifies as a civilian), but a member of the State's armed forces who performs no combat-related duties may be attacked at any time."[145] The ICRC comments on a similar inequity in an international armed conflict (IAC) are analogous:

it would contradict the logic of the principle of distinction to place irregular armed forces under the more protective legal regime afforded to the civilian population merely because they fail to distinguish themselves from that population, to carry their arms openly, or to conduct their operations in accordance with the laws and customs of war. Therefore, even under the terms of the Hague Regulations and the Geneva Conventions, all armed actors showing a sufficient degree of military organization and belonging to a party to the conflict must be regarded as part of the armed forces of that party.[146]

Likewise, it makes little sense for an ISIS member to receive protections that are not afforded to the military members of, say the Iraqi or U.S. military, who are not serving in a combat function during a NIAC.

Admittedly, this imbalance is not unique. In a NIAC, a State's armed forces will have a form of combatant immunity while the members of an OAG will not.[147] The United States expressly notes that "the non-State status of the armed group would not render inapplicable the privileges and immunities afforded lawful combatants and other State officials."[148] This difference is a result of the State being a sovereign while a non-State armed group, obviously, is not. [149] The inequity created by the CCF approach, though unfair to a State's armed forces, is therefore not without precedent. However, in contrast to the combatant immunity imbalance, which only adversely affects conflict participants, the CCF approach dangerously blurs the already murky line between civilians and fighters in a NIAC.[150] ,Both civilians and State armed forces are therefore disadvantaged by the narrow interpretation of OAG membership promoted by the CCF approach.

conflict.").

[145] Schmitt, *supra* note 6, at 132 (discussing how this approach skews the balance between military necessity and humanitarian considerations that undergirds all of LOAC.).

[146] ICRC INTERPRETIVE GUIDANCE, *supra* note 6, at 22. Although this interpretation represents the prevailing opinion of ICRC experts some concerns were expressed that this approach could be misunderstood as creating a category of persons protected neither by GC III nor by GC IV *Id*. at 22 fn 17.

[147] *See, e.g*., DOD LAW OF WAR MANUAL, *supra* note 6, at ¶ 17.4.1.1 ("persons belonging to non-State armed groups lack any legal privilege or immunity from prosecution by a State that is engaged in hostilities against that group"); UK MANUAL, *supra* note 73, at ¶ 15.6.3 (discussing consequences for a captured member of a dissident fighting force versus a member of the State's armed forces).

[148] DOD LAW OF WAR MANUAL, *supra* note 6, at ¶ 17.4.1.1.

[149] *Id*. at ¶ 17.4.1 ("the principle of the sovereign equality of States is not applicable in armed conflicts between a State and a non-State armed group."). *See also* Schmitt, *supra* note 6, at 133 (noting "the organized armed group lacks any domestic or international legal basis for participation in the conflict.").

[150] *See, e.g*., DOD LAW OF WAR MANUAL, *supra* note 6, at ¶ 17.5.1.1. (highlighting the difficulty in

Applying the CCF approach to ISIS thus has a number of dangerous consequences. In particular, it diminishes the protections for civilians and promotes inequality between ISIS's members and State armed forces. While the CCF concept was clearly developed with good intentions to avoid interpretations of OAG membership by "abstract affiliation, family ties, or other criteria prone to error, arbitrariness or abuse,"[151] in practice it fails to safeguard civilians.[152] As a result, it becomes apparent that a broader approach to determining OAG membership is necessary.

B. The Need for Targeting Flexibility

The conduct-link-intent test recognizes, and attempts to address, the problems resulting from the CCF approach to determining OAG membership. Unlike the CCF methodology, when applied to ISIS, this test would easily find that membership alone demonstrates intent to support the group's violent objectives. Both the first and second factors—tests of eligible conduct and associative links to the OAG—are theoretically possible to analyze by those conducting targeting activities against ISIS and could be described in appropriate ROE. Further, satisfying the third criteria—requiring an express finding of an individual's specific intent—is arguably already part of ISIS's strategy. The group often claims or endorses attacks by its "soldiers" "whether or not the individuals in question have been publicly shown to have a demonstrable operational link to, or history with, the organization."[153]

However, this novel approach presents two irreconcilable problems when applied on the modern battlefield. First, creating a criminal law statute-like list of qualifying conduct for OAG membership is inflexible and legalistic. Professor

identifying OAG members during a NIAC); Watkin, *supra* note 86, at 667 (noting that "it is difficult to see how allowing those providing direct support within an organized armed group to be protected by civilian status will actually operate to limit the conflict.").

[151] *See e.g.*, ICRC INTERPRETIVE GUIDANCE, *supra* note 6, at 33 (reasoning that establishing a continuous combat function is necessary due to the difficulty of distinguishing civilians in a NIAC); Schmitt, *supra* note 6, at 132 (noting that the CCF approach is theoretically justified).

[152] *See e.g.*, Watkin, *supra* note 86, at 675 ("A significant danger is presented to uninvolved civilians by an interpretation that would grant protected civilian status to persons who are an integral part of the combat effectiveness of an organized armed group when their regular force counterparts performing exactly the same function can be targeted."); VanLandingham, *supra* note 72, at 131–32. *See generally* YORAM DINSTEIN, THE CONDUCT OF HOSTILITIES UNDER THE LAW OF INTERNATIONAL ARMED CONFLICT 1 (2004).

> Some people, no doubt animated by the noblest humanitarian impulses, would like to see zero-casualty warfare. However, this is an impossible dream. War is not a chess game. Almost by definition, it entails human losses, suffering and pain. As long as it is waged, humanitarian considerations cannot be the sole legal arbiters of the conduct of hostilities.

Id.

[153] Blanchard & Humud, *supra* note 1, at 7.

VanLandingham pre-emptively addresses this critique and argues that such "perceived loss of flexibility is …a needed phenomenon to ensure appropriate breadth of membership."[154] Further, she notes that "surely no decision-maker today, when approving the addition of a new name to a targeting list based on the person's actions in relation to a particular group," would refute that the "individual in question does not possess a specific intent to further his terrorist group's violent means and ends by carrying out or giving group orders regarding the same."[155]

Yet, in the effort to expand OAG membership by arguing for an express list, targeting decisions are delayed. For example, ISIS consistently changes their routine behavior or conduct specifically to avoid being targeted by an opposing State actor, and issues guidance to its members on how to do so.[156] This behavior would undoubtedly require continual editing of both the categories of eligible conduct as well as any resultant individual targeting lists. These lists are a policy construct, not required by the LOAC, and would act as a limiting factor in the best of circumstances. Further, with ISIS at its peak in 2015 having tens of thousands of fighters,[157] and thousands more coming every month,[158] an element-based approach to targeting, in practical application, is unwieldy. While much of the territory ISIS held is now liberated, and its membership drastically decreased,[159] using an element-based approach to determining OAG membership remains impractical in both the contemporary[160] and future security environment.

The second problem with the conduct-link-intent test is found in the third criteria. Though not nearly as inequitable as the results from the CCF methodology, requiring a finding that an individual has the specific intent to further a group's violent ends provides additional protections for OAG members in comparison to a State's armed forces. Again, a member of a State armed force is targetable by virtue of their status. In comparison, the conduct-link-intent test requires an additional analytical step before targeting of an OAG member. As a

---

[154] VanLandingham, *supra* note 72, at 138.

[155] *Id*.

[156] *See* Keligh Baker, *Shave your beard, encrypt your phones and wear western clothes: ISIS issues booklet advising would-be terrorists how to avoid being spotted by Western security agencies*, DAILYMAIL.COM (Jan. 13, 2016, 6:24 PM), *http://www.dailymail.co.uk/news/article-3398424/ISIS-issues-booklet-advising-terrorists-avoid-spotted.html*.

[157] *See* Daveed Gartenstein-Ross, *How Many Fighters Does the Islamic State Really Have?*, WAR ON THE ROCKS (Feb. 9, 2015), https://warontherocks.com/2015/02/how-many-fighters-does-the-islamic-state-really-have/ (estimating the number of ISIS fighters as being closer to 100,000 than 30,000).

[158] *See Flow of foreign ISIS recruits much slower now, U.S. says*, CBS NEWS (Apr. 26, 2016, 1:02 PM), https://www.cbsnews.com/news/less-foreign-isis-recruits/ (reporting that approximately 1,500 foreign fighters came to Iraq and Syria a month in 2015 with the number decreasing to 200 a month in 2016).

[159] *See* Saphora Smith & Michele Neubert, *ISIS Will Remain A Threat in 2018, Experts Warn*, NBC News (Dec. 27, 2017, 3:17 AM), https://www.nbcnews.com/storyline/isis-terror/isis-will-remain-threat-2018-experts-warn-n828146.

[160] *Id*. (noting that ISIS is "far from defeated.").

result, an OAG member is treated more favorably than a member of a State's armed forces through the requirement for establishing specific intent.

C. If You Play the Game . . . Live With the Consequences

In comparison to the CCF approach, in our opinion the conduct-link-intent test better comports with the realities of the modern battlefield. Yet, as noted above, we consider this approach unnecessarily bureaucratic. What becomes apparent is that the broad approach to OAG membership allowed for by the conduct-link-intent test is appropriate as it is "unrealistic to expect government troops not to take measures against rebels simply because they are not involved in an attack."[161] However, what is also obvious is that this formalistic test is burdensome for commanders to implement. The best approach to determining OAG membership is therefore one that has the broad applicability of the conduct-link-intent test, but is also more operationally practical.

Simply treating organized armed groups and a State's armed forces the same accomplishes these goals.[162] First, this approach resolves the inequity and under-inclusivity issues presented by the CCF methodology and, in doing so, "not only reinforces the distinction principle but also recognizes that true civilian participation has to be limited in time and frequency so as not to undermine the protection associated with civilian status."[163] Second, it avoids mechanical, and consequently, restrictive tests for OAG membership. With the rise of powerful non-State actors, like ISIS, this straightforward and clear approach addresses the challenges of fighting in a contemporary NIAC by empowering commanders while also protecting civilians.

ISIS—organized, well-financed, and heavily armed—clearly acts and fights like a traditional military organization.[164] Again, not all that are affiliated with ISIS, or sympathetic to their cause, are part of the OAG. But those who are filling traditional military roles in ISIS should be subject to "attack so long as they remain active members of the group, regardless of their function."[165] Attaching the consequences of OAG membership to some of those in ISIS, and not others, ignores the realities of the modern battlefield.

---

[161] LINDSAY MOIR, THE LAW OF INTERNAL ARMED CONFLICT 59 (2002).

[162] Schmitt, *supra* note 6, at 133.

[163] Watkin, *supra* note 866, at 693.

[164] *See supra* text accompanying notes 44–64.

[165] Schmitt, *supra* note 6, at 133. *See also* VanLandingham, *supra* note 72, at 109 ("armed group membership, typically in a state military, produces a presumption of hostility, thereby making one a lawful target for elimination by opposing forces, even if one is not actually fighting. But this LOAC targeting axiom is not limited to state militaries. It extends to non-state armed groups as well . . . .")

CONCLUSION

So, again, is the brother of the ISIS Commander described in the opening hypothetical vignette targetable? Yes. He has affirmatively proclaimed his loyalty to the group, and his actions as the "public face" of ISIS are arguably no different than those of a Public Affairs Officer serving in a State's armed forces.[166] Clearly, he is under command serving in a traditional military role making him a member of the group. Consequently, he is subject to the adverse consequences of his status, including being a lawful target.

One of the greatest attributes of the LOAC is its "emphasis on being applied equally to all participants."[167] Focusing on the membership structure of an OAG reinforces this aspect of the law. Doing otherwise "creates a bias against State armed forces, making its members much easier to target while imposing on them more exacting criteria when targeting opponents."[168] Additionally, protection of civilians is "one of the main goals of international humanitarian law."[169] Emphasizing function over membership also dangerously blurs the line between civilians and fighters, undercutting this principle. Both of these are untenable results. Of course, any approach to determining membership must also be practical. An expansive understanding of who qualifies as a member of an OAG resolves these outstanding concerns and is necessary in the current conflict environment.

---

[166] *See* U.S. Army, *Careers & Jobs Public Affairs Officer (46A)*, GoArmy.com, https://www.goarmy.com/careers-and-jobs/browse-career-and-job-categories/arts-and-media/public-affairs-officer.html (last visited Mar. 13, 2018) (describing some of the responsibilities of a Public Affairs Officer as "gain[ing] the support of the American public," "respond to media queries," "develop and execute communication plans," as well as other internal and external communication activities.)

[167] Watkin, *supra* note 86, at 695.

[168] *Id*. at 688, 694 ("In many circumstances, waiting for an act to be carried out may leave security forces with insufficient time to react, thereby actually increasing the risk to civilians . . . .")

[169] *See* ICRC INTERPRETIVE GUIDANCE, *supra* note 6, at 4 ("The protection of civilians is one of the main goals of international humanitarian law.")

REVISITING BELLIGERENT REPRISALS IN THE AGE OF CYBER?

DAVID WALLACE, SHANE REEVES & TRENT POWELL*

I. INTRODUCTION

With respect to current and future warfare, it is virtually impossible to exaggerate the significance of information technology. Today's armed forces use a host of weapons, munitions, and systems that function through the operation of highly sophisticated information systems.[1] For instance, the command and control of operational forces are increasingly coordinated and directed through computer-based networks that allow for real-time sharing of information and common pictures of the battlespace.[2] Moreover, logistics, at all levels of warfare, are entirely at the mercy of information systems. And, of

* Colonel David Wallace is the Professor and Head, Department of Law, United States Military Academy at West Point, New York. In 2017, Colonel Wallace served as a Visiting Scholar at the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn, Estonia. The author would like to thank the NATO CCDCOE Director, Merle Maigre, the Law Branch Chief, Lauri Aasmann, and all of the members of the Law Branch for their collegial assistance and support during the fellowship. Lieutenant Colonel Shane Reeves is the Professor and Deputy Head, Department of Law, United States Military Academy at West Point, New York. He is an Associate Professor of Law. Major Trent Powell is serving as an action officer in the Future Concepts Directorate at The Judge Advocate General's Legal Center & School. Major Powell previously served as an Assistant Professor of Law, Department of Law, United States Military Academy at West Point, New York. The opinions, conclusions, and recommendations in this article do not necessarily reflect the views of the Department of Defense, the United States Army, or the United States Military Academy.

1. COMM. ON OFFENSIVE INFO. WARFARE, NAT'L RESEARCH COUNCIL OF THE NAT'L ACADS., TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 9 (William A. Owens et al. eds., 2009).

2. *Id.*

course, in recent years the development of cutting edge, high-tech cyber weapons allow for an attack against an adversary in both virtual and real domains.[3] While this "New Age of Cyber" may seem to raise questions about the legal framework applicable to the conduct of such operations, the traditional normative legal structure for warfare, the *jus ad bellum*[4] and the *jus in bello*,[5] still regulate the actions of belligerents engaged in cyber hostilities.

This article deals with legal issues in the cyber warfare context related to the *jus in bello*, which is also referred to as international humanitarian law (IHL). The international legal community acknowledges and widely accepts that IHL applies to cyber operations undertaken in the context of an armed conflict.[6] The challenge, of course, is not that IHL applies, but rather how it specifically applies to cyber operations. Unquestionably, digital means and methods of warfare executed in both the virtual and real world pose novel issues.[7] In this regard, it is necessary to consider and examine how pre-cyber IHL laws, as well as the values that formed the foundation for those laws,[8] translate into regulation of armed conflicts in the New Age of Cyber. Although there are many issues and topics that are worthy of such a re-examination, few are as controversial as the notion of belligerent reprisals under IHL.

As will be discussed in detail below, a belligerent reprisal under IHL is a method of warfare that is otherwise unlawful but, in exceptional cases, is lawful when used as an enforcement mechanism in response to unlawful enemy acts.[9] As noted by Professor William Schabas, "[r]eprisal amounts to an argument that crimes are justifiable as a proportionate response to criminal acts committed by the other party. In a sense, it is the most ancient means of

3. *Id.* at 10.

4. *Jus ad bellum* addresses when a State may use force under international law. *What are* Jus ad bellum *and* Jus in bello*?* INT'L COMM. RED CROSS, https://www.icrc.org/en/document/what-are-jus-ad-bellum-and-jus-bello-0 [https://perma.cc/7AP3-7D8M] (last visited Nov. 7, 2017). Some legal commentators have observed that the United Nations Charter creates a legal regime more accurately characterized as *jus contra bellum* because it is fundamentally devised to prevent the use of force. *See* ROBERT KOLB & RICHARD HYDE, AN INTRODUCTION TO THE INTERNATIONAL LAW OF ARMED CONFLICTS 13 (2008).

5. The *jus in bello* regulates the conduct of parties engaged in an armed conflict. *See What are Jus ad bellum and Jus in bello?*, *supra* note 4.

6. *See* TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 3 (Michael N. Schmitt ed., 2017) [hereinafter TALLINN MANUAL 2.0].

7. *See, e.g.*, David Wallace & Shane R. Reeves, *The Law of Armed Conflict's "Wicked" Problem:* Levée en Masse *in Cyber Warfare*, 89 INT'L L. STUD. 646, 666–67 (2013) (discussing the difficulty of applying the traditional IHL interpretation of a *levée en masse* in the cyber domain).

8. HEATHER HARRISON DINNISS, CYBER WARFARE AND THE LAWS OF WAR 239–40 (James Crawford & John S. Bell eds., 2012).

9. 1 JEAN-MARIE HENCKAERTS & LOUISE DOSWALD-BECK, CUSTOMARY INTERNATIONAL HUMANITARIAN LAW: RULES 513 (2005).

enforcement of the law."[10] Under this assertion, then, a "proportionate response" by an aggrieved party serves as a *jus in bello* enforcement of the law. And, because the enforcement of international law and IHL specifically, is the obvious shortcoming with international law, belligerent reprisals may provide a timely mechanism to redress enemy violations of IHL *during* the armed conflict itself.[11]

The use of belligerent reprisal has evolved over time "from a fundamental and nearly universally recognized aspect of the international law" regulating warfare "into a complex and [highly] contentious sanction."[12] Arguably, in modern IHL, reprisals have been largely—but not entirely—prohibited by customary and codified law. The 1977 Additional Protocols (AP) I[13] is unquestionably the international community's strongest and most comprehensive condemnation of belligerent reprisals as a method of warfare. Commenting on the efforts that led to AP I, Konstantin Obradovic, who took part in the Diplomatic Conference of 1974–1977 as a member of the Yugoslav delegation, made the following observations about belligerent reprisals:

> With its well-nigh absolute prohibition of reprisals against all categories of protected persons who fall into enemy hands, Protocol I goes further down the trail blazed in 1949. The underlying considerations are both humanitarian and rational. The history of war—and the Second World War in particular—clearly shows that, apart from being barbarous, unfair and inequitable as they invariably victimize the innocent, reprisals achieve nothing. Even if they are 'justified' as a response to enemy violation of the law, they never result in the triumph of the rule of law. Moreover, all the mass executions of the last world war, all the Oradour-sur-Glane of this world have not been enough to dampen people's determination to resist. Reprisals therefore appear pointless.[14]

10. GARY D. SOLIS, THE LAW OF ARMED CONFLICT: INTERNATIONAL HUMANITARIAN LAW IN WAR 693 (2d ed. 2016) (quoting WILLIAM A. SCHABAS, THE INTERNATIONAL CRIMINAL COURT: A COMMENTARY ON THE ROME STATUTE 496 (2010)).

11. A.P.V. ROGERS, LAW ON THE BATTLEFIELD 14 (2d ed. 2004). Importantly, reprisals are separate and distinct from acts of retaliation and revenge, which remain unlawful under IHL. GEOFFREY BEST, HUMANITY IN WARFARE 19 (1980).

12. Sean Watts, *Reciprocity and the Law of War*, 50 HARV. INT'L L.J. 365, 382 (2009).

13. Protocols Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts, Jun. 8, 1977, 1125 U.N.T.S. 3 [hereinafter Protocol I].

14. Konstantin Obradovic, *The Prohibition of Reprisals in Protocol I: Greater Protection for War Victims*, INT'L REV. RED CROSS, Oct. 31, 1997, at 524, https://www.icrc.org/eng/resources/documents/article/other/57jnv7.htm [https://perma.cc/FY6J-PF9P].

While Obradovic expressed this view at the earliest period in the development of cyber capabilities, the current and future state of reprisals in the cyber realm require a review of more recent legal analysis. In that regard, a useful starting point for legal practitioners, policymakers, non-governmental organizations,[15] cyber security professionals, military commanders, and scholars is the 2017 *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (*Tallinn Manual 2.0*).[16] This resource, which is best understood as the collective opinions of a group of international experts, helpfully addresses the question of belligerent reprisals under IHL in armed conflict as well as many other vital issues spanning public international law in its nearly 600 pages of highly informative text.[17] Impressively, *Tallinn Manual 2.0* has 154 rules including two rules on reprisals: Rule 108, *Belligerent Reprisals*, and Rule 109, *Reprisals under Additional Protocol I*.[18] In addition to the actual rules contained in *Tallinn Manual 2.0*, the manual provides detailed commentary, offering some tremendously valuable insights into the normative context of the rules as well as practical implications for their application.[19] Finally, and most importantly, it is important to note that the experts who wrote *Tallinn Manual 2.0* were limiting themselves to an objective restatement of the *lex lata* and scrupulously avoided including statements reflecting the *lex ferenda*.[20]

This article critically explores the legal landscape of belligerent reprisals and considers whether the use of these measures is a viable enforcement mechanism under IHL in the context of cyber operations. Because of the layered approach to this inquiry, the article has seven parts that build upon each other. Part II of the article provides an overview of the history of belligerent reprisals under IHL. Part III discusses belligerent reprisals in the context of today's understanding of IHL. Part IV further explores cyber operations and belligerent reprisals: the *lex lata*. Countermeasures (at one time known as peacetime reprisals) under the law of state responsibility forms the basis of Part V. Part VI provides an analytical framework for considering how cyber means

15. An example of one such non-governmental organization is the ICRC. *The ICRC's Mandate and Mission*, INT'L COMM. RED CROSS, https://www.icrc.org/en/mandate-and-mission [https://perma.cc/XQM3-32BJ] (last visited Dec. 6, 2017). The ICRC is an "independent, neutral organization ensuring humanitarian protection and assistance for victims of armed conflict and other situations of violence. It takes action in response to emergencies and at the same time promotes respect for international humanitarian law and its implementation in national law." *Id.*

16. TALLINN MANUAL 2.0, *supra* note 6.

17. *See id.*

18. *Id.* at 460–63.

19. *Id.* at 3–5.

20. *Id.* at 3.

and methods could effectively facilitate an expanded use of belligerent reprisals for some States under some conditions. Additionally, this section serves as the lens for re-examining the propriety and practicality of breathing life back into this controversial enforcement mechanism under IHL. Lastly, Part VII summarizes and concludes the article.

II. THE HISTORY OF BELLIGERENT REPRISALS IN IHL

Reprisals have been the traditional method of enforcement of IHL since at least the late nineteenth and early twentieth centuries.[21] This time period saw a number of advances in IHL including the adoption of the first Geneva Convention; the St. Petersburg's Declaration, which renounced the use of exploding bullets projectiles under 400 grams; and the drafting and implementation of the so-called Lieber Code[22] during the American Civil War.[23] The 1863 Lieber Code addressed the concept of reprisals throughout its 157 articles.[24] Notably, Francis Lieber, the Code's main architect and drafter, described "retaliation"—which was used synonymously with the term "reprisals"—as the sternest feature of war.[25] Article 28 of the Code states:

> Art. 28. Retaliation will, therefore, never be resorted to as a measure of mere revenge, but only as a means of protective retribution, and moreover, cautiously and unavoidably; that is to say, retaliation shall only be resorted to after careful inquiry into the real occurrence, and the character of the misdeeds that may demand retribution. Unjust or inconsiderate retaliation removes the belligerents farther and farther from the mitigating rules of regular war, and by rapid steps leads them nearer to the internecine wars of savages.[26]

During the American Civil War reprisals were a lawful method of enforcing the laws and customs of war with both sides making abundant use of the method.[27] The Lieber Code even permitted retaliation against prisoners of war

21. HENCKAERTS & DOSWALD-BECK, *supra* note 9, at 514.

22. SOLIS, *supra* note 10, at 44–45. In 1862, the War Department appointed a board of officers, including Francis Lieber, to propose a "Code of Regulations for the government of armies in the field." *Id*. The military officers on the board worked primarily on a revision to the Articles of War. *Id*. Francis Lieber, a professor at Columbia, wrote the Code that bears his name. *Id*. In 1863, President Lincoln directed that Lieber's 157-article Code be incorporated into the Union Army's General Orders as "General Order 100." *Id*.

23. *Id*. at 43.

24. *See* General Orders No. 100: Instructions for the Government Armies of the United States in the Field (Apr. 24, 1863) [hereinafter *Lieber Code*].

25. *Id*. art.27.

26. *Id*. art.28.

27. Patryk I. Labuda, *The Lieber Code, Retaliation and the Origins of International Criminal*

("[a]ll prisoners of war are liable to the infliction of retaliatory measures.").[28] In only the instance of later capture and execution of deserters joining an enemy army did the Lieber Code forbid retaliation.[29]

Despite the Lieber Code's statement on the lawfulness of reprisals, other legal bodies sought to limit the use of reprisals. The Brussels Conference of 1874 and the Institute of International Law meeting at Oxford in 1880 were two such instances.[30] The Institute's Manual of the Laws of War on Land stated that reprisals "must conform in all cases to the laws of humanity and morality."[31] However, the Hague Conventions at the turn of the twentieth century did not prohibit the use of belligerent reprisals apart from providing some rudimentary protections for prisoners of war.[32] In fact, during early armed conflicts of the twentieth century, air attacks were a legitimate means and method of reprisal against a defaulting enemy to bring it back to its senses.[33] Commenting on this phenomenon, Air Commodore William Boothby stated:

> The civilian population and the popular press would demand retaliatory or reprisal action against the enemy in response to air raids that occasioned civilian loss. Air raids carried out as reprisal action could be portrayed by the adverse party as simple illegal acts ignoring, of course, the alleged prior illegality cited as justifying the reprisal in the first place.[34]

Reprisals in World War I caused much hardship for the victims of the conflict and, in particular, prisoners of war. As a result, the idea of prohibiting all reprisals against prisoners of war gained traction, eventually finding official endorsement in special agreements concluded between parties to the conflict

---

Law, *in* 3 HISTORICAL ORIGINS OF INTERNATIONAL CRIMINAL LAW 299, 304, 306 (Morten Bergsmo et al. eds., 2015).

28. *Lieber Code*, *supra* note 24, art.59.

29. *Id.* art.48. This provision specifically states:

> Deserters from the American Army, having entered the service of the enemy, suffer death if they fall again into the hands of the United States, whether by capture, or being delivered up to the American Army; and if a deserter from the enemy, having taken service in the Army of the United States, is captured by the enemy, and punished by them with death or otherwise, it is not a breach against the law and usages of war, requiring redress or retaliation.

Id.

30. *See* Project of an International Declaration Concerning the Laws and Customs of War, Brussels, Aug. 27, 1874, https://ihl-databases.icrc.org/ihl/INTRO/135 [https://perma.cc/Q5VC-QGC8]; The Laws of War on Land, Oxford, Sept. 9, 1880, https://ihl-databases.icrc.org/ihl/INTRO/140?OpenDocument [https://perma.cc/M2FJ-AG3G].

31. The Laws of War on Land, *supra* note 30, art.86.

32. INGRID DETTER, THE LAW OF WAR 301 (2d ed. 2000).

33. WILLIAM H. BOOTHBY, THE LAW OF TARGETING 512 (2012).

34. *Id.* at 512–13.

towards the end of the war.[35] Following World War I, the 1929 Geneva Convention on Prisoners of War began the process of gradually excluding groups of persons and civilians' property from the scope of reprisals,[36] including prisoners of war.[37] Commenting on this particular category, Michael Walzer, in his classic book *Just and Unjust Wars*, stated, "prisoners were singled out because of the implied contract by surrender, in which they are promised life and benevolent quarantine. Killing them would be a breach of faith as well as a violation of the positive laws of war."[38]

Despite these efforts, World War II saw the regular use of reprisals by the parties to the conflict.[39] There were a number of well-known incidents involving reprisals including one involving the Germans and the French resistance fighters in 1944.[40] After the Normandy invasion, French resistance fighters organized into the French Forces on the Interior (FFI) and began operating openly and on a larger scale.[41] They wore insignia visible at a distance, carried their arms openly, and abided by the laws and customs of war, thereby qualifying them as lawful combatants.[42] However, the Germans did not recognize the FFI as lawful combatants.[43] Rather, the Germans viewed them as criminals and summarily executed a number of FFI fighters upon capture.[44]

By the late summer of 1944, "many German soldiers had surrendered to the FFI."[45] When the FFI learned the Germans executed eighty FFI fighters and planned to execute more, "the FFI announced that it would carry out eighty reprisal executions."[46] The International Committee of the Red Cross (ICRC)

35. Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, Aug. 12, 1949, 6 U.S.T. 3114, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Comment.xsp?action=openDocument&documentId=8F88DE5EE5DEA183C12563CD0042207D [https://perma.cc/P7T2-57TR].

36. THE HANDBOOK OF INTERNATIONAL HUMANITARIAN LAW 234 (Dieter Fleck ed., 3d ed. 2013).

37. Convention Relative to the Treatment of Prisoners of War, Geneva, July 27, 1929, Art. 2, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/ART/305-430003?OpenDocument [https://perma.cc/244B-DFX9].

38. MICHAEL WALZER, JUST AND UNJUST WARS: A MORAL ARGUMENT WITH HISTORICAL ILLUSTRATIONS 209 (4th ed. 2006).

39. DETTER, *supra* note 32, at 301.

40. Kenneth Anderson, *Reprisal Killings*, *in* CRIMES OF WAR 2.0: WHAT THE PUBLIC SHOULD KNOW 358, 358–59 (Roy Gutman, David Rieff & Anthony Dworkin eds., 2007).

41. *Id*. at 358.

42. *Id.*

43. *Id.*

44. *Id.*

45. *Id.*

46. *Id.*

intervened and sought to postpone the executions pending an agreement whereby the Germans would recognize the FFI as lawful combatants.[47] But, after six days in which the Germans did not respond, the FFI executed eighty German prisoners.[48] Subsequently, the historical accounts indicate the Germans abandoned any plans to execute additional FFI prisoners.[49]

In addition to the actual use of reprisals by parties in World War II, there was also the threatened use of belligerent reprisals. For example, President Franklin Roosevelt threatened the use of retaliatory attacks upon becoming aware that Axis forces sought to use poison gas.[50] The regular use, or threat of use, of belligerent reprisals in World War II thus became an important topic in the post-war tribunals. Commenting about the scope of belligerent reprisals, the International Military Tribunal found that:

> The right of reprisals against civilians was restricted by rules laid down in the judgments of the Military Tribunal at Nuremberg. The Tribunal emphasised that reprisals must at least be limited geographically to one area, mainly as action against persons in one area could have little deterrent effect on people in other areas. If there was not such geographical connection a 'functional' link might be acceptable as limiting the right of reprisals: there had thus to be some connection between the reprisals and the civilians against whom action was taken. The Tribunal furthermore ruled out reprisals for which certain ethnic, religious or political groups had been selected.[51]

On August 12, 1949, a diplomatic conference in Geneva approved the text of four conventions to which more States have ratified than any other international agreements in the laws regulating armed conflict: the 1949

47. *Id.*

48. *Id.*

49. *Id.*

50. Andrew D. Mitchell, *Does One Illegality Merit Another? The Law of Belligerent Reprisals in International Law*, 170 MIL. L. REV. 155, 171 (2001). President Roosevelt specifically stated:

> [T]here have been reports that one or more of the Axis powers were seriously contemplating use of poisonous or noxious gases or other inhumane devices of warfare. . . . We promise to any perpetrators of such crimes full and swift retaliation in kind. . . . Any use of gas by any Axis power, therefore, will immediately be followed by the fullest possible retaliation upon munition centers, seaports, and other military objectives throughout the whole extent of the territory of such Axis country.

Id. (alteration in original).

51. DETTER, *supra* note 32, at 301.

Geneva Conventions.[52] The Conventions were, in part, born out of the unprecedented brutality and violence of World War II.[53] As Ambassador George H. Aldrich commented:

> The history of development of this branch of international law is largely one of reaction to bad experience. After each major war, the survivors negotiate rules for the next war that they would, in retrospect, like to have seen in force during the last war. The 1929 and 1949 Geneva Conventions attest to that pattern.[54]

The four Conventions prohibited belligerent reprisals with respect to the specific classes of individuals covered by each agreement: wounded, sick, and shipwrecked; medical and religious personnel; prisoners of war; civilians in occupied territories; as well as certain objects such as medical facilities and supplies and private property of civilians in occupied territory.[55] Adding to

52. ADAM ROBERTS & RICHARD GUELFF, DOCUMENTS ON THE LAWS OF WAR 195 (3d ed. 2000). To provide some background and context, the Geneva Conventions may be traced back to a well-to-do Swiss businessman, Henri Dunant, and the Battle of Solferino in 1859. *Solferino and the International Committee of the Red Cross*, INT'L COMM. RED CROSS, https://www.icrc.org/eng/resources/documents/feature/2010/solferino-feature-240609.htm [https://perma.cc/KC3E-SDEH] (last visited Jan. 3, 2018). The Battle of Solferino in Lombardy, not far from Milan and Verona, was fought between the forces of Austria and a French-Piedmontese alliance. *Id*. The battle was one of the bloodiest of the nineteenth century with thousands of dead and wounded on both sides. *Id*. The military practice of the time was to leave the wounded where they had fallen on the battlefield. *Id*. Dunant was there and witnessed the carnage and participated in the aftermath attempting to provide aid and comfort to survivors. *Id*. Dunant could not forget what he saw and experienced. *Id*. He published in 1862 a small book, *A Memory of Solferino*. *Id*. In the book, Dunant vividly and graphically described the battle and the suffering of the wounded and injured soldiers. *Id*. Additionally, in the book, Dunant called for the creation of relief societies in each country that would act as auxiliaries to the army medical services to facilitate the care for all wounded and sick, whichever side they were on. *Id*. This effort led eventually to the formation of the International Committee of the Red Cross. *Id*. Also, as part of Dunant's vision in *A Memory of Solferino*, he proposed that an international principle be created to serve as the basis for these societies. *Id*. Dunant's idea ultimately led to the Swiss government hosting an official diplomatic conference in August 1864, which resulted in the adoption of the first Geneva Convention. *Id*. In 1901, Dunant was awarded the first-ever Nobel Peace Prize for what was accurately described as the "supreme humanitarian achievement of the 19th century." *Id*.

53. *See* Phillip Spoerri, Dir. of Int'l Law, Int'l Comm. of the Red Cross, Address at Ceremony to Celebrate 60th Anniversary of the Geneva Conventions: The Geneva Conventions of 1949: Origins and Current Significance (Dec. 8, 2009), https://www.icrc.org/eng/resources/documents/statement/geneva-conventions-statement-120809.htm [https://perma.cc/2QXP-FPQ8].

54. SOLIS, *supra* note 10, at 88.

55. THE HANDBOOK OF INTERNATIONAL HUMANITARIAN LAW, *supra* note 36, at 234, 334.

these prohibitions, the 1954 Hague Convention on the Protection of Cultural Property prohibited reprisals against objects protected under the convention.[56]

The 1977 AP I significantly enlarged the traditional prohibitions of reprisals under IHL adding several other categories of prohibited reprisal targets.[57] In addition to a general prohibition, AP I also specifically prohibits reprisals against the civilian population and objects; cultural property and places of worship; objects indispensable to the survival of the civilian populations; the natural environment; and works or installations containing dangerous forces.[58] However, the United States, as well as several other States, objected to these additional restrictions on reprisals as being counterproductive.[59]

Specifically, the United States argued AP I's greater prohibition on reprisals removed a significant tool for protecting civilians and war victims on all sides of a conflict.[60] For example, article 51 of the Protocol "prohibits any reprisal attacks against the civilian population, that is, attacks that would otherwise be forbidden but that are in response to the enemy's own violations of the law and are intended to deter future violations."[61] Yet, historically, reprisals were the major sanction underlying the laws of war and ensured reciprocal compliance.[62] "If article 51 were to come into force for the United States, an enemy could deliberately carry out attacks against friendly civilian populations, and the United States would be legally forbidden to reply in kind."[63] As a result, "[t]o formally renounce even the option of such attacks" would "remove a significant deterrent" for those intent on targeting unfriendly

56. *Id*. at 434; *see also* Hague Convention for the Protection of Cultural Property in the Event of Armed Conflict, May 14, 1954, 249 U.N.T.S. 240, 244–48.

57. TALLINN MANUAL 2.0, *supra* note 6, at 463.

58. *Id.*

59. GEOFFREY S. CORN ET AL., THE LAW OF ARMED CONFLICT: AN OPERATIONAL APPROACH 227 (2012). In fact, the United States's objections concerning reprisals was one of the reasons it did not ratify AP I. *See* SOLIS, *supra* note 10, at 128–38; *see also* Michael J. Matheson, Deputy Legal Adviser, U.S. Dep't of State, Remarks at American Red Cross-Washington College of Law Conference on International Humanitarian Law (Jan. 22, 1987), *in* 2 AM. U. J. INT'L L. & POL'Y 419, 426 (1987).

60. OFFICE OF THE GEN. COUNSEL, U.S. DEP'T OF DEF., DEPARTMENT OF DEFENSE LAW OF WAR MANUAL § 18.18.3.4, at 1088–89 (2016) [hereinafter LAW OF WAR MANUAL].

61. *Id*. § 18.18.3.4, at 1089 n.221 (quoting Judge Abraham D. Sofaer, Legal Adviser, U.S. Dep't of State, Remarks at American Red Cross-Washington College of Law Conference on International Humanitarian Law (Jan. 22, 1987), *in* 2 AM. U. J. INT'L L. & POL'Y 460, 469 (1987)).

62. *See* Watts, *supra* note 12, at 382.

63. LAW OF WAR MANUAL, *supra* note 60, § 18.18.3.4, at 1089 n.221 (quoting Sofaer, *supra* note 61, at 469).

civilian populations.[64] Today, the United States continues to hold, as an option, the use of reprisals in limited circumstances.[65]

III. BELLIGERENT REPRISALS TODAY IN IHL

As is evident from the above, the historical development of reprisals under IHL established a gradual trend to outlaw the practice.[66] There are, however, several important considerations with respect to reprisals under the present IHL framework. First, as a threshold matter, to the degree that a reprisal would be lawful today, they are subject to stringent controls.[67] Second, the concept of belligerent reprisals exists in the context of international armed conflicts and not in non-international armed conflicts.[68] And third, under customary IHL, there are six general conditions precedent to lawfully employing belligerent reprisals.[69]

The first condition relates to the purpose of reprisals.[70] As mentioned previously, the use of reprisals is only in reaction to a prior serious violation of IHL and done for the purpose of inducing the enemy to comply with IHL.[71] In many respects, this is the *sine qua non* of reprisals, i.e., to induce a law-breaking State to abide by IHL in the future.[72] Of course, in practice, determining motive for particular actions may be problematic. That is, it may be very difficult to discern whether there is a legitimate purpose for an action, i.e., inducing an adversary to comply with the law, or whether an act is actually retaliation, retribution, or revenge.[73] Additionally, because of the underlying purpose of belligerent reprisals, anticipatory or counter reprisals are impermissible.[74]

The second condition is that the employment of belligerent reprisals is a matter of last resort, and there must be no other lawful measures available to induce the enemy to respect and comply with IHL.[75] Before using reprisals,

64. *Id.* (quoting Sofaer, *supra* note 61, at 469).

65. *See* CORN ET AL., *supra* note 59, at 227.

66. HENCKAERTS & DOSWALD-BECK, *supra* note 9, at 513–14.

67. *Id.* at 513.

68. TALLINN MANUAL 2.0, *supra* note 6, at 464. The ICRC, in Rule 148 of its Customary International Law Study takes the position that parties to non-international armed conflicts do not have the right to resort to belligerent reprisals. *See* HENCKAERTS & DOSWALD-BECK, *supra* note 9, at 526.

69. HENCKAERTS & DOSWALD-BECK, *supra* note 9, at 515–18; *see also* LAW OF WAR MANUAL, *supra* note 60, § 18.18.2.5, at 1086.

70. HENCKAERTS & DOSWALD-BECK, *supra* note 9, at 515.

71. *Id.*

72. *Id.* at 515–16.

73. BEST, *supra* note 11, at 167.

74. HENCKAERTS & DOSWALD-BECK, *supra* note 9, at 515.

75. *Id.* at 516.

States must first attempt to secure the enemy's compliance with IHL through certain means.[76] For example, actions such as "protests and demands, retorsion, or reasonable notice of the threat to use reprisals" are necessary before resorting to belligerent reprisals.[77] Notably, both international and domestic courts require meeting this condition prior to utilizing reprisals.[78]

The third condition is proportionality.[79] Proportionality has multiple meanings in international law. Generally, within the context of customary IHL, proportionality is understood to mean that an attack is prohibited if the incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, is "excessive in relation to the concrete and direct military advantage anticipated."[80] By contrast, in the context of belligerent reprisals, most State practices illustrate that the acts taken in reprisal be proportionate to the original violation, free from the balancing approach under the prevalent proportionality notion.[81]

In practice, proportionality may be hard to gauge in nature and scope, although it does not mean equivalence. Rather, it should be construed to mean the response should not be excessive.[82] Additionally, it is important to note that the proportionality requirement does not mean that the belligerent reprisal needs to be in kind.[83] For example, if State A bombs civilian objects in State B, State B is not limited to only bombing civilian objects in State A. In fact, there are many scenarios where there is not a direct counterpart to the original violation or the victim State may simply lack the technical expertise to respond in the same fashion.[84]

The fourth condition is somewhat straightforward and self-explanatory. Because reprisals are significant military and political acts that require careful and complex judgments, the law withholds authority to exact reprisals to the highest levels of government within a State.[85] As noted by one legal commentator about this unusual, but important condition:

> Because of the extremely complex legal and political assessment which must precede any reprisal, it is necessary

76. YORAM DINSTEIN, THE CONDUCT OF HOSTILITIES UNDER THE LAW OF INTERNATIONAL ARMED CONFLICT 221 (2004).

77. LAW OF WAR MANUAL, *supra* note 60, § 18.18.2.2, at 1085.

78. HENCKAERTS & DOSWALD-BECK, *supra* note 9, at 516.

79. *Id.* at 517.

80. LAW OF WAR MANUAL, *supra* note 60, § 2.4.1.2, at 61.

81. HENCKAERTS & DOSWALD-BECK, *supra* note 9, at 518.

82. DINSTEIN, *supra* note 76, at 221.

83. *Id.*

84. *Id.*

85. HENCKAERTS & DOSWALD-BECK, *supra* note 9, at 518.

> that the political leadership of a belligerent state decide on any possible use of reprisals. The exact legal nature of the adverse belligerent's actions may be extremely difficult to determine; even more importantly, a decision to use reprisals requires a genuine assessment of the political risks as well as the immediate dangers connected with the use of a reprisal.[86]

The fifth condition is intuitive and consistent with the overarching purpose of reprisals. Under this requirement, reprisal actions must immediately cease as soon as the enemy complies with IHL.[87] This condition is consistent with and highlights the nature of reprisals as a deterrent measure. Finally, the sixth condition prior to using reprisals is that in order to fulfil their purpose, dissuade an adversary from further unlawful conduct, and to promote adherence to IHL, States must announce the action and make it public.[88]

Beyond these six, strictly legal considerations, there are also several practical consequences before resorting to the use of belligerent reprisals. First, resorting to belligerent reprisals may ultimately divert valuable and scarce military resources.[89] Second, since belligerent reprisals are, by definition, violations of international norms, other States may not only disagree with the decision to use them, but also view their use as a violations of IHL and subject to sanction.[90] Third, it is very possible the use of reprisals may strengthen an adversary's morale and will to resist.[91] Fourth, many observers view reprisals as a "race to the bottom," leading to a vicious cycle of counter-reprisals.[92] Finally, like other serious violations of IHL, the use of belligerent reprisals may exacerbate tensions between the parties to the conflict making it more difficult for them to end the armed conflict and return to a peaceful state.[93] Given the legal framework as outlined above, coupled with a number of compelling practical considerations, belligerent reprisals are seemingly a waning IHL enforcement mechanism. Yet, the New Age of Cyber is challenging many seemingly settled areas of international law and therefore it is worth discussing the validity of belligerent reprisals during cyber operations.

86. THE HANDBOOK OF INTERNATIONAL HUMANITARIAN LAW, *supra* note 36, at 228.

87. HENCKAERTS & DOSWALD-BECK, *supra* note 9, at 518.

88. LAW OF WAR MANUAL, *supra* note 60, § 18.18.2.5, at 1086.

89. *Id.* § 18.18.4, at 1090.

90. *Id.*

91. *Id.*

92. *Id.*

93. *Id.*

IV. CYBER OPERATIONS AND BELLIGERENT REPRISALS: THE *LEX LATA*

As a starting point, when thinking about the *lex lata*, it is important to reiterate that the applicable IHL treaties were drafted before cyberspace and operations were a reality.[94] Likewise, there are many challenges associated with the emergence of customary IHL cyber-related norms with the most notable being the highly classified nature of cyber activities by States.[95] However, it is also important to note, as discussed above, it is widely accepted that IHL applies to cyber operations in the context of an armed conflict.[96] With that said, the *Tallinn Manual 2.0* Rules and Commentary provide a valuable resource and assist in identifying issues, gaps, and ambiguities in the law. But, when thinking about the *lex lata*, it is always important to be mindful of whether application of traditional rules of IHL make sense when applied in the cyber context.

This acknowledgment includes the possible use of belligerent reprisals with Rule 108 of *Tallinn Manual 2.0*, which provides basic parameters for use during cyber operations in an international armed conflict. The Rule notes that belligerent reprisals are expressly prohibited against "prisoners of war; interned civilians, civilians in occupied territory or otherwise in the hands of an adverse party to the conflict, and their property; those *hors de combat*; and medical and religious personnel, facilities, vehicles, and equipment."[97] In other circumstances, where international law does not prohibit use "belligerent reprisals are subject to stringent conditions."[98]

The Commentary to Rule 108 provides granularity into the experts' conclusions concerning belligerent reprisals. The experts state, unequivocally, that cyber reprisals are prohibited against the wounded, sick, or shipwrecked; medical personnel, units, establishments, or transports; chaplains; prisoners of war, or interned civilians and civilians in the hands of an adverse party who are protected by the Fourth Geneva Convention, or their property.[99] In effect, these prohibitions are customary international law that binds all States. However, the

94. DINNISS, *supra* note 8, at 239, 241.

95. TALLINN MANUAL 2.0, *supra* note 6, at 377.

96. *Id.* at 3. When one thinks of the use of cyber in the context of an armed conflict, it involves not only the employment of cyber capabilities to objectives in and through cyberspace, but also involves requirements such as weapons reviews to ensure that cyber means of warfare that are acquired or used complies with the law of armed conflict. *Id.* at 375; Michael N. Schmitt & Liis Vihul, *The Emergence of International Legal Norms for Cyberconflict*, *in* BINARY BULLETS: THE ETHICS OF CYBERWARFARE 34, 49 (Fritz Allhoff, Adam Henschke & Bradley Jay Strauser eds., 2016).

97. TALLINN MANUAL 2.0, *supra* note 6, at 460.

98. *Id.*

99. *Id*. at 461.

experts disagreed as to whether customary international law protected cultural property.[100]

Further outlining the proper use of belligerent reprisals in the cyber context, and particularly how AP I's greater prohibitions apply, is Rule 109 of *Tallinn 2.0.* The Rule, rooted in seven different provisions found in AP I, states:

> Additional Protocol I prohibits States Parties from making the civilian population, individual civilians, civilian objects, cultural property and places of worship, objects indispensable to the survival of the civilian population, the natural environment, and dams, dykes, and nuclear electrical generating stations the object of a cyber-attack by the way of reprisal.[101]

The commentary to Rule 109 expands on the general prohibition of cyber reprisals against the aforementioned categories by those States that are parties to AP I and engaged in an international armed conflict.[102] But, the commentary suggests the prohibition is conditional for certain States that adopted understandings during the ratification of AP I.[103] And, despite certain international tribunals holding reprisals against civilians a violation of customary international law, this practice has yet to "crystallise" into a customary rule due to contrary practice.[104] Nevertheless, in substance, the *Tallinn Manual 2.0* experts found that AP I dramatically reduces the use of reprisals in cyber operations by limiting use to only against enemy armed forces, their facilities, and equipment.[105]

Tallinn Manual 2.0's Rule 108, Rule 109, and associated commentary provide an excellent summary of the current law concerning belligerent reprisals in the cyber context. Clearly, the *Tallinn Manual 2.0* agrees that belligerent reprisals have limited use in the contemporary environment as an IHL enforcement mechanism. However, a comparison between belligerent reprisals and the concept of countermeasures under international law may indicate it is time to revisit this determination in the New Age of Cyber. It is important to note that such an intellectual and academic thought experiment, i.e., comparing countermeasures and belligerent reprisals, should not be taken to conflate or confuse these two distinct enforcement mechanisms under international law. They are very different. The common ground between the

100. *Id.* at 463.

101. *Id.*

102. *Id.* at 463–64.

103. *Id.*

104. *Id.* at 464.

105. CORN ET AL., *supra* note 59, at 227. *See generally* KOLB & HYDE, *supra* note 4, at 195.

two is in their underlying purpose and that alone warrants the comparison below.

V. COUNTERMEASURES UNDER INTERNATIONAL LAW

In the first half of the twentieth century, so-called countermeasures were referred to as "peacetime reprisals."[106] Although belligerent reprisals and countermeasures apply under different circumstances, their purpose is fundamentally the same: to force a State that violates international law to discontinue illegal activity.[107] In this respect, countermeasures provide a good point of comparison with belligerent reprisals.

As a threshold matter, it is important to note that States are responsible for their internationally wrongful acts under the law of State responsibility.[108] Article 2 of the International Law Commission's *Articles of State Responsibility for Internationally Wrongful Acts*[109] provides as follows:

> Article 2
> Elements of an internationally wrongful act of a State
>
> There is an internationally wrongful act of a State when conduct consisting of an action or omission:
>
> (a) is attributable to the State under international law; and
> (b) constitutes a breach of an international obligation of the State.[110]

106. Michael N. Schmitt, *Cyber Activities and the Law of Countermeasures*, *in* PEACETIME REGIME FOR STATE ACTIVITIES IN CYBERSPACE: INTERNATIONAL LAW, INTERNATIONAL RELATIONS AND DIPLOMACY 659, 662 (Katharina Ziolkowski ed., 2013). The term peacetime is no longer used.

107. *Id.* at 661–62.

108. *Id.* at 661.

109. Int'l Law Comm'n, Rep. on the Work of Its Fifty-Third Session, U.N. Doc. A/56/10, (2001), http://www.un.org/law/ilc/ [https://perma.cc/9838-MCGV] [hereinafter Articles on State Responsibility]. Beginning in 1956, the Articles of State Responsibility for Internationally Wrongful Acts were drafted over decades by the International Law Commission. The 59 Articles are divided into four parts: Part One (The Internationally Wrongful Act of the State, articles 1–27); Part Two (Content of the International Responsibility of a State, articles 28–41); Part Three (The Implementation of the International Responsibility of a State, articles 42–54); and Part Four (articles 55–59) contains the final five General Provisions of the text. Although the Articles are not binding, they are authoritative because the International Law Commission developed them over decades under the leadership of multiple special rapporteurs. Schmitt, *supra* note 106, at 661.

110. James Crawford, THE INTERNATIONAL LAW COMMISSION'S ARTICLES ON STATE RESPONSIBILITY: INTRODUCTION, TEXT AND COMMENTARIES 81 (2002). As noted in the commentary to Article 2, the element of attribution is sometimes described as "subjective" while the element of a breach is referred to as "objective"; *see* Articles on State Responsibility, *supra* note 109, at 34.

The breach of an international obligation may consist of a violation of a treaty, customary international law, or of general principles of law.[111] For example, internationally wrongful acts may include a cyber operation that violates the sovereignty of another State or the principle of non-intervention among other things. [112] A well-known recent example of an international wrongful act involved the Russian interference in the 2016 U.S. presidential election.[113] According to Professor Michael Schmitt, "Russia's apparent attempt to influence the outcome of the election by its release of emails through WikiLeaks probably violates the international law barring intervention in a state's internal affairs."[114] Another example may be a State that conducts cyber operations against a coastal State from a ship located in the territorial waters of the injured State. These actions would breach international law proscribing innocent passage found in the *United Nations Convention on* the *Law of the Sea*.[115]

One possible consequence for a state that chooses to commit an international wrongful act is entitling a targeted state to resort to countermeasures.[116] "Countermeasures are actions by an injured State that breach obligations owed to the 'responsible' State (the one initially violating its legal obligations) in order to persuade the latter to return to a state of lawfulness."[117] Countermeasures are therefore different than either a retorsion or a plea of necessity. Retorsions are actions taken by a State that are best

111. Articles on State Responsibility, *supra* note 109, at 35.

112. TALLINN MANUAL 2.0, *supra* note 6, at 312–13.

113. *See Russian Hacking and Influence in the U.S. Election*, N.Y. TIMES, https://www.nytimes.com/news-event/russian-election-hacking [https://perma.cc/3FFS-PADV] (last visited Apr. 3, 2018).

114. Ellen Nakashima, *Russia's Apparent Meddling in U.S. Election is Not an Act of War, Cyber Expert Says*, WASH. POST (Feb. 7, 2017), www.washingtonpost.com/news/checkpoint/wp/2017/02/07/russias-apparent-meddling-in-u-s-election-is-not-an-act-of-war-cyber-expert-says/?utm_term=.0e23dfb985de [https://perma.cc/SU9Q-MYGM].

115. Schmitt, *supra* note 106, at 664–65.

116. *See* Int'l Law Comm'n, Rep. on the Work of Its Fifty-Fifth Session, U.N. Doc. A/58/10, at 75 (2003), http://www.un.org/law/ilc/ [https://perma.cc/57YV-NKTX] [hereinafter Articles on State Responsibility II] ("The wrongfulness of an act of a State not in conformity with an international obligation towards another State is precluded if and to the extent that the act constitutes a countermeasure taken against the latter State in accordance with chapter II of Part Three.").

117. Michael Schmitt, *International Law and Cyber Attacks: Sony v. North Korea*, JUST SECURITY (Dec. 17, 2014), http://justsecurity.org/18460/international-humanitarian-law-cyber-attacks-sony-v-north-korea/ [https://perma.cc/CN2H-5JRZ]; *see also* TALLINN MANUAL 2.0, *supra* note 6, at 111 (describing countermeasures as "actions or omissions by an injured State [in response to internationally wrongful acts] directed against a responsible State that would violate an obligation owed by the former to the latter.").

described as unfriendly, but not inconsistent with an international obligation of a State.[118] An example includes limitations upon normal diplomatic relations or other contacts, embargos of various kinds, or withdrawal of voluntary aid programs.[119] A plea of necessity, on the other hand, denotes exceptional cases where a State, faced with grave and imminent peril to an essential interest, takes measures counter to its international obligations to safeguard those particular interests.[120] In the cyber context, an example of the circumstances leading to a plea of necessity may involve a cyber operation against a State's critical infrastructure.[121] In contrast to either a retorsion or a plea of necessity, a countermeasure allows "a state victimized by another . . . to use acts traditionally prohibited under international law to force the offending state to comply with their legal obligations."[122]

In describing countermeasures in a cyber context, Professor William Banks commented that "[c]ountermeasures are responses, whether cyber in nature or not, below the use of force threshold designed to prevent or mitigate a perpetrator State from continuing its unlawful cyber intervention."[123] In this regard, countermeasures are similar to belligerent reprisals in that they allow a State to act unlawfully in order to force international legal compliance.[124] Of course there are differences between the two—countermeasures only apply below the use of force threshold, are limited in severity,[125] and must not involve the threat or use of force[126]—whereas belligerent reprisals only apply during an international armed conflict and would otherwise violate IHL but for a prior illegal act.[127] Nevertheless, despite these differences, countermeasures provide

118. Schmitt, *supra* note 117.

119. *Id.*

120. DINNISS, *supra* note 8, at 102.

121. Schmitt, *supra* note 106, at 663.

122. Daniel Garrie & Shane R. Reeves, *So You're Telling Me There's a Chance: How the* Articles on State Responsibility *Could Empower Corporate Responses to State-Sponsored Cyber Attacks*, HARV. NAT'L SECURITY J. ONLINE FEATURES 5 (2015), http://harvardnsj.org/wp-content/uploads/2016/01/Garrie-and-Reeves-Non-State-Actor-and-Self-Defense.pdf [https://perma.cc/SY6X-W7PR].

123. William Banks, *State Responsibility and Attribution of Cyber Intrusions After* Tallinn 2.0, 95 TEX. L. REV. 1487, 1501 (2017).

124. Schmitt, *supra* note 106, at 662. As noted by Professor Schmitt, the idea of a reprisal was also thought of in a *jus ad bellum* context. That is, "[t]he historical notion of reprisals was broader than that of countermeasures in that it included both non-forceful and forceful actions. Today, forceful reprisals have been subsumed into the U.N. Charter's use of force paradigm, which allows States to resort to force in response to armed attacks." *Id.*

125. Articles on State Responsibility II, *supra* note 116, at 129.

126. *Id.* at 131. *See generally* TALLINN MANUAL 2.0, *supra* note 6, at 38.

127. Schmitt, *supra* note 106, at 662.

a valuable lens by which to view belligerent reprisals in the context of cyber operations. Accordingly, there are four features of countermeasures worth highlighting: (1) the purpose of countermeasures; (2) restrictions or limitations on their use; (3) proportionality; and (4) attribution standards.

The purpose of a countermeasure is to return a situation to a condition of lawfulness[128] by inducing a State, who is responsible for internationally wrongful acts, to comply with its obligations and where appropriate make assurances or guarantees and reparations. Rule 21 of *Tallinn Manual 2.0* further speaks to the purpose of countermeasures in the context of cyber. It provides that "[c]ountermeasures, whether cyber in nature or not, may only be taken to induce a responsible State to comply with the legal obligations it owes an injured State."[129] Furthermore, by definition, countermeasures are a reactive, remedial, self-help measure necessitated by a lack of a compulsory dispute resolution mechanism, and are a product of a decentralized system by which an aggrieved State may seek to vindicate its rights and restore a proper legal relationship with the responsible State.[130]

It is important to note, however, that countermeasures are not intended as punishment.[131] Yet, like other forms of self-help, countermeasures are subject to abuse, especially between States of unequal power.[132] And, similar to belligerent reprisals, it may be difficult to distinguish the precise motive for pursuing the countermeasure. In other words, a pertinent question is whether countermeasures exacted against a State are being done to induce the State, who is responsible for internationally wrongful acts, to comply, or is it being done in retaliation, retribution, or revenge? In answering this question, if the countermeasure will only exacerbate a situation, it is likely a fair indication the motive may be rooted more in retaliation.[133]

The second inquiry involves restrictions on the use of countermeasures. The most significant restriction stems from the use of force as proscribed by

128. *Id.* at 674.

129. TALLINN MANUAL 2.0, *supra* note 6, at 116. Speaking to the underlying mind set of countermeasures "should be a wager on the wisdom, not on the weakness of the other Party. They should be used with a spirit of great moderation and be accompanied by a genuine effort at resolving the dispute." *Case Concerning the Air Service Agreement of 27 March 1946 Between the United States of America and France*, 18 U.N. REP. INT'L ARBITRAL AWARDS 417, 445. One particular risk in the context of cyber is the speed at which cyber operations may unfold, both intentionally wrongful acts and countermeasures, may detract from careful consideration of intent and consequences.

130. Schmitt, *supra* note 106, at 662; DINNISS, *supra* note 8, at 281.

131. Schmitt, *supra* note 106, at 674.

132. *Id.*

133. TALLINN MANUAL 2.0, *supra* note 6, at 117.

Article 2(4) of the United Nations Charter.[134] Articles 49 and 50 of the *Articles of State Responsibility for Internationally Wrongful Acts* further define the limits of the legal boundaries on the use of countermeasures.[135] Under Article 49, constraints exist on a countermeasure's object and purpose and are limited to the responsible State's period of non-performance of its international obligations.[136] Additionally, as far as possible, countermeasures must be taken in such a way to permit the resumption of performance of the obligation in question.[137] Article 50 expands on the foregoing by specifying a number of international obligations the performance of which may not be impaired by countermeasures.[138] Drawing from Article 50, *Tallinn Manual 2.0*, Rule 22 provides that "[c]ountermeasures, whether cyber in nature or not, may not include actions that affect fundamental human rights, amount to prohibited belligerent reprisals, or violate peremptory norm. A State taking countermeasures must fulfil its obligations with respect to diplomatic and consular inviolability."[139]

The third inquiry when considering the use of countermeasures involves the notion of proportionality.[140] Article 51 of the *Articles of State Responsibility* provides that "[c]ountermeasures must be commensurate with the injury[141] suffered, taking into account the gravity of the internationally wrongful act and the rights in question."[142] Much like the "purpose" of countermeasures,

134. U.N. Charter art. 2, ¶ 4. This provision also reflects customary international law. As noted by Professor Schmitt, the dilemma lies in determining when a cyber operation qualifies as a use of force thereby making it impermissible as a countermeasure. *See* Schmitt, *supra* note 106, at 678.

135. Articles on State Responsibility II, *supra* note 116, at 129–34.

136. *Id.* at 129.

137. *Id.*

138. *Id.* at 131.

139. TALLINN MANUAL 2.0, *supra* note 6, at 122–23.

140. It is important to note that proportionality with respect to countermeasures is separate and distinct from the concept of proportionality in *jus ad bellum* or IHL. With respect to *jus ad bellum*, the concept of proportionality considers the degree of force necessary for a State to defend itself against an armed attack. In that context, proportionality serves to identify the circumstances in which the unilateral use of force is permissible under international law. Additionally, it also serves to determine the intensity and the magnitude of military operations. In the context of IHL, proportionality means essentially whether an attack shall be cancelled or suspended if the attack may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof. *See* Protocol I, *supra* note 13, art. 51, at 37, art. 57, at 41–42.

141. Articles of State Responsibility II, *supra* note 116, at 134. "Injury" means a breach of an international legal obligation. It should not be understood to require damage. *See* TALLINN MANUAL 2.0, *supra* note 6, at 127.

142. Articles of State Responsibility II, *supra* note 116, at 134; DINNISS, *supra* note 8, at 103–04. The principle of proportionality is a deeply rooted requirement for countermeasures and is widely recognized in State practice, doctrine and international jurisprudence. For example, in the *Naulilaa* case, using the word "reprisal," the court stated, "Even if one admitted that international law does not

proportionality is also an essential limitation on the injured State in terms of the employment of specific countermeasures and the level of their intensity.[143] A countermeasure that is disproportionate amounts to an impermissible punishment or retaliation, and is contrary to the object and purpose of countermeasures.[144] A proportionality analysis provides a check on the potentially escalating effect of countermeasures and is a control on the exercise of "decentralized power conferred on States to react individually to international wrongful acts."[145] However, it is important to note that proportionality does not mean or imply reciprocity.[146] In fact, it is entirely lawful to use non-cyber countermeasures in responses to an internationally wrongful act involving cyber operations.[147]

In the context of cyber, it is feasible to narrowly tailor the intensity, duration, and effects of the operation. For example, a cyber operation aimed at incapacitating infrastructure without destroying it may be particularly useful in meeting the limitations on countermeasures, including proportionality.[148] Noting the challenges of assessing proportionality in the context of countermeasures, *Tallinn Manual 2.0* states, in part:

> The interconnected and interdependent nature of cyber systems can render it difficult to determine accurately the consequences likely to result from cyber countermeasures. States must therefore exercise considerable care when assessing whether their countermeasures will be proportionate. Conducting a full assessment may require, for instance, mapping the targeted system or reviewing relevant intelligence. Whether the assessment is adequate depends on the foreseeability of potential consequences and the feasibility of means that can be used to conduct it.[149]

The final issue with respect to countermeasures concerns attribution. The issue of attribution includes more than technically determining the source of the

require that the reprisal be approximately measured by the offense, one should certainly consider as excessive, and thus illegal, reprisals out of all proportion with the act which motivated them." Naulilaa Incident Arbitration, Portuguese-German Arbitral Tribunal, 1928, *reprinted and translated in* WILLIAM W. BISHOP, JR., INTERNATIONAL LAW: CASES AND MATERIALS 903, 904 (3d ed. 1971).

143. DINNISS, *supra* note 8, at 104.

144. TALLINN MANUAL 2.0, *supra* note 6, at 127.

145. JAMES CRAWFORD, STATE RESPONSIBILITY: THE GENERAL PART 698 (James Crawford & John S. Bell eds., 2013).

146. *See* DINNISS, *supra* note 8, at 104.

147. TALLINN MANUAL 2.0, *supra* note 6, at 128.

148. MARCO ROSCINI, CYBER OPERATIONS AND THE USE OF FORCE IN INTERNATIONAL LAW 106 (2014).

149. TALLINN MANUAL 2.0, *supra* note 6, at 128.

attack. It also includes policy and legal issues. The difficulties in attributing cyber-attacks and determining the identity of the perpetrators causes a perception that States can operate with virtual impunity in the cyber realm.[150] The various tools, tactics, and techniques available to conceal cyber activities compounds the challenges to attribute attacks to States, non-State actors, or individuals.[151] For example, a responsible State may gain "control of another State's cyber infrastructure and use it to mount harmful" attacks against a third State.[152] This situation illustrates the technical complexities that exist in the cyber domain. While future technological innovations may mitigate the attribution obstacle, "as with any forensic investigation, information gathering" in cyberspace is likely to remain technically challenging, time consuming, and resource intensive.[153]

While ascertaining the source of a cyber-attack remains problematic, some influential thought leaders have challenged the paradigmatic thinking that discovering the point of attack and those individuals responsible is necessary for the purpose of attribution.[154] Proponents of this concept disagree that once the technical forensics of the attack is established only then can attribution hope to determine the person or organization responsible for it.[155] Instead, they conceptualize the problem of attribution as one to consider in the light of this question: What do national policy leaders actually need to know about the cyber operation?[156] In answering this question, national leaders should simply know who is ultimately responsible for the attack rather than who actually committed the acts.

An example of this distinction between determining responsibility versus identifying the actual perpetrators occurred in 1999 when NATO inadvertently bombed the Chinese embassy in Belgrade during the armed conflict in Kosovo.[157] In the aftermath of the tragedy, scores of people gathered in Beijing near the U.S. Embassy, including many students bused in for the protests.[158]

150. Michael N. Schmitt & Liis Vihul, *Proxy Wars in Cyberspace: The Evolving International Law of Attribution*, FLETCHER SECURITY REV., Spring 2014, at 53, 54 (2014).

151. Schmitt, *supra* note 106, at 685.

152. *Id.*

153. Louise Arimatsu, *Classifying Cyber Warfare*, *in* RESEARCH HANDBOOK ON INTERNATIONAL LAW AND CYBERSPACE 326, 333 (Nicholas Tsagourias & Russell Buchan eds., 2015).

154. Jason Healy, *The Spectrum of National Responsibility for Cyberattacks*, BROWN J. WORLD AFF., Fall/Winter 2011, at 57, 57 (2011).

155. *Id.*

156. *Id.*

157. *Id.* at 58.

158. *Id.*

Despite protesters pummeling the U.S. Embassy with bricks and rocks,[159] U.S. authorities did not seek to identify the individual stone throwers "because the exact attribution was not an important input for decision makers."[160] The United States knew that the Chinese were responsible for attacks regardless of who threw the individual rocks.[161] Even though knowing who actually threw the rocks would provide many data points, that information would not be particularly helpful to deciding how to respond to the incident.[162] Similarly, with cyber-attacks, it is often not necessarily probative who actually initiated the attack at the lowest technical level.[163] Instead, the most important determination is who is overall responsible. In sum, reconceptualizing the concept of attribution may serve to provide decision-makers with flexibility to respond in the complex domain of cyber.[164]

Countermeasures have become an important tool, even if not used, for States to force compliance with international law in cyber space below the use of force threshold.[165] Taking the foregoing background into consideration, countermeasures are, in many respects, the other side of the belligerent reprisal coin. It is therefore worth asking whether belligerent reprisals may serve an equally useful purpose as countermeasures when addressing cyber operations in the international armed conflict context.

159. *Chinese in Belgrade, Beijing Protest NATO Embassy Bombing*, CNN (May 9, 1999, 9:44 PM), http://edition.cnn.com/WORLD/asiapcf/9905/09/china.protest.03/ [https://perma.cc/E6EG-QQZF].

160. Healy, *supra* note 154, at 58.

161. *Id.*

162. *Id.*

163. *Id.* at 57.

164. Attribution also presents challenging legal and factual issues. For example, what are the evidentiary considerations when using countermeasures? The Commentary to the *Articles on State Responsibility* suggest the standard for factual attribution is identification with responsible certainty, *see* Schmitt, *supra* note 106, at 685, and, importantly, only States may use countermeasures. TALLINN MANUAL 2.0, *supra* note 6, at 130. This restriction thus precludes private firms, like Sony for instance, from engaging in "hack-back" countermeasures against North Korea after a cyber-attack in 2014. *See generally* David E. Sanger, David D. Kirkpatrick & Nicole Perlroth, *The World Once Laughed at North Korean Cyberpower. No More.*, N.Y. TIMES (Oct. 15, 2017), https://www.nytimes.com/2017/10/15/world/asia/north-korea-hacking-cyber-sony.html [https://perma.cc/985U-TXV8]. *But see generally* Garrie & Reeves, *supra* note 122, at 13 (discussing a possible way for a corporation to use countermeasures).

165. *See, e.g.*, Nakashima, *supra* note 114 (noting that the United States most likely has grounds to use countermeasures against Russia for the 2016 election hacking actions) (quoting Professor Michael Schmitt).

VI. BELLIGERENT REPRISALS AND CYBER: A THEORETICAL FRAMEWORK

Sir Hersch Lauterpacht, one of the leading international lawyers of the twentieth century, observed that "[i]f international law is, in some ways, at the vanishing point of law, the law of war is, perhaps even more conspicuously, at the vanishing point of international law."[166] At some level, Lauterpacht's insightful remarks are not surprising in that IHL is attempting to regulate the worst of human conditions—war. International Humanitarian Law seeks to introduce moderation and restraint into a pursuit defined by violence and death, unbridled passion and hatred, as well as confusion and unpredictability. At its best, IHL is never more than imperfectly observed, and at its worst, very poorly observed.[167] Commenting on the effectiveness of the *jus in bello*, distinguished British historian Geoffrey Best stated, "[w]e should perhaps not so much complain that the law of war does not work well, as marvel that it works at all."[168] Unquestionably, Best is absolutely correct in his assessment. Yet, beyond the substance and circumstances of what IHL attempts to regulate, there is another factor that places international law generally, and IHL specifically, at the "vanishing point of law"—anemic enforcement mechanisms.

The challenges in enforcing and implementing norms are a significant reason why international law faces enduring criticism. Arguably, meaningful enforcement is the Achilles heel of this area of law, especially if "law" is the commands of a sovereign backed by sanctions as articulated by legal positivists from Hobbes to Austin.[169] Furthermore, critics have long contended the intractable problem of meaningful enforcement and sanctions in international law not only undermines the effectiveness and credibility of the international normative system, but also suggests whether international law is "law" at all if it cannot be imposed.[170] Even then, one has to be careful not to overstate the problem and place international law in the proper context:

> The international situation cannot be equated to the situation within states. There is not a powerful international body that has authority over the subjects of the law; the international community does not have an international police force and a

166. BEST, *supra* note 11, at 12.

167. *Id.* at 11.

168. *Id.* at 12.

169. Jack Goldsmith & Daryl Levinson, *Law for States: International Law, Constitutional Law, Public Law*, 122 HARV. L. REV. 1791, 1822 (2009).

170. Elena Katselli Proukaki, *The Problem of Enforcement in International Law: Countermeasures, the Non-Injured State and the Idea of International Community*, INT'L L. OBSERVER (May 18, 2010, 11:23 AM), http://www.internationallawobserver.eu/2010/05/18/the-problem-of-enforcement-in-international-law-countermeasures-the-non-injured-state-and-the-idea-of-international-community [https://perma.cc/S9UZ-6EW6].

> judiciary with compulsory jurisdiction; thus, coercive power exercised by the international community cannot be relied upon to enforce international obligations. The sovereignty and equality of states precludes the operation of such mechanisms, and ensures that the execution of the law is precarious and, sometimes, irregular.[171]

Although difficulties exist in enforcing IHL, there are some mechanisms for enforcement including protecting powers,[172] fact finding commissions,[173] penal sanctions,[174] and reparations.[175] But, challenges still remain. The absence of a hierarchical system or institution capable of enforcement, implementation, and accountability fundamentally precludes IHL's decentralized character from undergoing meaningful change in the foreseeable future. So, how should the international community respond when confronted with the realities of international law? Do advances in technology provide an opportunity to better promote lawfulness on the modern battlefield? In the context of cyber and the emergence of new capabilities, revisiting belligerent reprisals provides a means to overcome the obvious challenges underlying the enforcement of IHL.

One way to conceptualize or consider the issue of belligerent reprisals is to think of them as three points on a left-to-right continuum. At the far left end of the continuum, the first category, are belligerent reprisals that should never

171. KOLB & HYDE, *supra* note 4, at 283.

172. Under IHL, a "protecting power" is a neutral, third-party State designated as a party to the conflict and accepted by the enemy party. This State has agreed to carry out the functions assigned to a protecting Power under IHL. These functions include monitoring and ensure compliance with the law. In the absence of an agreement, the ICRC or any other impartial humanitarian organization may designate a protecting power substitute. Notably, the use of this system is rare in recent years. *See Protecting Powers: How Does the Law Protect in War?*, INT'L COMM. RED CROSS, https://casebook.icrc.org/glossary/protecting-powers [https://perma.cc/CZ47-2G5G] (last visited Jan. 26, 2018).

173. Article 90 of the 1977 Additional Protocol I provides for the establishment of an International Fact-Finding Commission. Established in 1991, it is a permanent body of 15 independent experts acting in their personal capacity. The Commission's purpose is to contribute to implementation of and ensure respect for IHL in armed conflicts. Thilo Marauhn, *The International Humanitarian Fact Finding Commission—Dedicated to Facilitating Respect for International Humanitarian Law*, INT'L HUMANITARIAN FACT-FINDING COMM'N, www.ihffc.org/index.asp?Language=EN&page=home [https://perma.cc/8YXN-9DHV] (last visited Jan. 26, 2018).

174. International Humanitarian Law is enforceable in both domestic courts and international tribunals. Over the last three decades there has been significant efforts internationally to prosecute war crimes in ad hoc tribunals like the International Criminal Tribunals for the former Yugoslavia and Rwanda as well as the International Criminal Court.

175. HUMA HAIDER, GSDRC, INTERNATIONAL LEGAL FRAMEWORKS FOR HUMANITARIAN ACTION: TOPIC GUIDE 49 (2013), http://www.gsdrc.org/topic-guides/international-legal-frameworks-for-humanitarian-action/challenges/compliance-with-and-enforcement-of-ihl/ [https://perma.cc/FF3Z-XKFX].

occur regardless of the motive, means, or method. For example, belligerent reprisals against persons under the control of a party to the conflict should never be the target of a reprisal. As a representative list, this would include the following category of individuals: "prisoners of war; interned civilians, civilians in occupied territory or otherwise in the hands of an adverse party to the conflict, and their property; those *hors de combat*; and medical and religious personnel, facilities, vehicles, and equipment."[176]

This first category also contains certain objects immune as targets of reprisals, including medical buildings, vessels, or equipment; works or installations containing dangerous forces; objects indispensable to the survival of the civilian population; and cultural property and places of worship.[177] Furthermore, the belligerent reprisals continuum precludes the use of chemical or biological weapons.[178] Certain cyber operations that would fit into the above category include opening the flood gates of a dam causing the release of a body of water capable of widespread destruction; or, using a cyber-attack to target a hospital by turning off its electricity or taking some action to remotely taint the food or water supply for the civilian population.

There are a number of reasons to categorically exclude the foregoing belligerent reprisals. First, attacking these persons and objects are simply too inhumane and barbaric. If IHL seeks to balance between the meta-principles of military necessity and humanity, the above egregious and irreversible acts may never been offset by necessity. The second reason goes to the underlying purpose of belligerent reprisals, i.e., to induce an adversary to comply with IHL. The above examples will likely cause an escalation in violence by inflaming passions and resentments, leading additional violations of IHL and continued hostilities. Third, using countermeasures as an analogy, these actions are neither reversible nor likely to induce a return to lawfulness. Instead, the harshness of the acts make them more analogues to punishments and retaliation, and whether exacted in the cyber realm or not, these belligerent reprisals should be categorically banned.

At the far right end of the continuum are belligerent reprisals that do not shock the conscience and, in the gritty world of pragmatism, are reasonable and rational responses to induce an adversary's compliance with IHL.[179] To some that take an absolutist approach to reprisals, the suggestion that there is any place on the continuum for belligerent reprisals is cause for great concern. But,

176. TALLINN MANUAL 2.0, *supra* note 6, at 460.

177. Mitchell, *supra* note 50, at 162–64.

178. LAW OF WAR MANUAL, *supra* note 60, § 18.18.3.4, at 1088.

179. Michael A. Newton, *Reconsidering Reprisals*, 20 DUKE J. COMP. & INT'L L. 361, 361 (2010).

even the ICRC in their 2005 *Study on Customary International Humanitarian Law* did not take the position that there is a complete ban on belligerent reprisals.[180] Rule 145 of the *Study* stated, "Where not prohibited by international law, belligerent reprisals are subject to stringent conditions."[181]

An example at this end of the spectrum may involve the use of a prohibited weapon against combatants or military objectives.[182] For example, suppose a State is a party to the Convention on Cluster Munitions[183] or Ottawa Convention[184] and uses cluster munitions or antipersonnel mines as a belligerent reprisal against another State party. Assuming, *arguendo*, that the other criteria for a belligerent reprisal are met, such an action is permissible.[185] For somewhat obvious reasons, the parallel to countermeasures would be the strongest in this type of case.

Tallinn Manual 2.0 provides a hypothetical to illustrate a lawful cyber operation for those States not a party to 1977 AP I.[186] In the scenario, the armed forces of one State bomb the medical facilities of another State in the context of an armed conflict and the victim State is not a party to AP I.[187] In response, and after repeated demands to cease the bombings, the Prime Minister of the victim State approves a cyber-attack against a power generation facility used exclusively to provide power to the civilian population.[188] The purpose of this cyber reprisal operation is to compel the State which was attacking the medical facilities to stop.[189] So long as the Prime Minister orders the cessation of cyber-attacks as soon as the aggressive state stops attacking its medical facilities, the reprisal is legal according to the *Tallinn Manual 2.0* experts.[190]

The middle of the continuum is the most important to this analysis and one where the employment of cyber means and methods are legitimate so long as their purpose is to induce an adversary to be in compliance with IHL and so long as they are tailored to mitigate some of negative and collateral effects. It

180. HENCKAERTS & DOSWALD-BECK, *supra* note 9, at 513.

181. *Id.*

182. WILLIAM H. BOOTHBY, WEAPONS AND THE LAW OF ARMED CONFLICT 54 (2009).

183. THE CONVENTION ON CLUSTER MUNITIONS, www.clusterconvention.org/ [https://perma.cc/FM5T-XBZ4] (last visited Oct. 21, 2018).

184. *Anti-Personnel Landmines Convention*, UNITED NATIONS OFF. GENEVA, www.un.org/disarmament/geneva/aplc/ [https://perma.cc/G3M3-AWNE] (last visited Oct. 21, 2018).

185. BOOTHBY, *supra* note 182, at 54.

186. TALLINN MANUAL 2.0, *supra* note 6, at 462.

187. *Id.*

188. *Id.*

189. *Id.*

190. *Id.* The Experts did note that if the belligerent reprisal involved attacking the other State's medical facilities that would be considered unlawful under *Tallinn Manual 2.0*, Rule 108.

is important to reiterate that the ability to develop and execute belligerent reprisals in the middle of the continuum depends, in part, on whether the State is a party to AP I as seen in the example above. The United States, again, is not a party to AP I with one of the primary reasons being the wide-ranging prohibitions against reprisals.[191] The United States' position in this case stemmed from its concern about what could lawfully be done immediately to stop an enemy State from violating IHL.[192]

So, what are the likely objects a State may attack as a belligerent reprisal that would be considered in the middle of the continuum? So long as a State meets all the criteria as outlined above in Part III,[193] reprisals may include a cyber operation against a portion of a State's economic infrastructure such as communication and transportation networks, financial markets, or energy sectors.[194] These reprisals would need to be narrowly tailored such that they cause disruption, inconvenience or, in some cases, perhaps reversible non-permanent damage to a target.[195] Additionally, using a reprisal to target the civilian leadership of a State in order to exploit damaging personal and professional information may induce a State adversary to comply with IHL. This is a non-exhaustive list of potential targets for a cyber reprisal and are best viewed as illustrating the middle of the continuum. However, what becomes apparent is that through the use of cyber belligerent reprisals a State can meaningfully enforce IHL compliance without causing repugnant and irreparable harm. Of course, further discussion on the reconceptualization of cyber belligerent reprisals is necessary to provide greater clarity on the middle of the continuum.

Viewing cyber reprisals along this continuum provides decision-makers the flexibility of options to respond in a lawful manner against a belligerent State while also remedying the shortcoming of enforcing IHL. While belligerent reprisals have been generally discarded by the international community, and justifiably so, cyber operations warrant a re-examination of this tool for IHL enforcement. A dialogue between States on this possibility would be a worthy endeavor.

VII. CONCLUSION

In sum, the employment of belligerent reprisals is a course of action with wide-ranging implications and should never be undertaken lightly.

191. Matheson, *supra* note 59, at 420.

192. SOLIS, *supra* note 10, at 132.

193. *See supra* notes 66–93 and accompanying text.

194. ROSCINI, *supra* note 148, at 104.

195. *Id.* at 106.

Nevertheless, they are lawful acts if approved at the highest levels of government with the purpose to compel an adversary to comply with IHL. Using this ancient enforcement mechanism provides a means to overcome the anemic deficiency of enforcing IHL. Although there have been efforts to impose meaningful international penal sanctions in the past few decades, much more needs to be done *during* the armed conflict itself to ensure compliance. As illustrated in this article, cyber means and methods create opportunities to compel an adversary to comply with IHL while, at the same time, mitigating the effects of cyber operations.

Some well-intentioned individuals and groups may summarily dismiss belligerent reprisals because of the horrific abuses and risks associated with their use. But, viewing countermeasures as a conceptual backdrop in terms of purpose and limitations, the time has come to at least consider the possibilities at the intersection of IHL and emerging technologies. As uncivilized, repugnant, and archaic as it may seem, strictly controlled reprisals may be justifiable as a proportionate response to the criminal acts committed by an adversary to prompt compliance with the law. Emerging cyber means and methods may be the right tool at the right time to do just that.