CONFLICT CLASSIFICATION AND CYBER OPERATIONS: GAPS, AMBIGUITIES AND FAULT LINES

DAVID A. WALLACE* & CHRISTOPHER W. JACOBS**

ABSTRACT

This Article examines whether the conflict classification paradigm for international humanitarian law ("IHL") established by the 1949 Geneva Conventions is adequate to regulate armed conflicts that center, in whole or in part, on cyber operations. The analysis herein, presented in seven parts, answers that question affirmatively, but posits that the advent of cyber operations has exposed certain gaps, ambiguities, and fault lines in IHL's conflict classification framework. After the Introduction, Part II provides four examples of situations of violence—three of which amount to armed conflicts under IHL and one that does not meet the definitional criteria of armed conflict under IHL. Part III gives an overview of conflict classification under IHL. Parts IV and V examine international and non-international armed conflicts, respectively. Part VI highlights four overarching tensions between IHL's conflict classification and cyber operations.

---

* Colonel Wallace is a Professor and Head of the Department of Law, United States Military Academy. Wallace served as a Visiting Scholar at the North Atlantic Treaty Organization ("NATO") Cooperative Cyber Defence Centre of Excellence (CCD COE) in Tallinn, Estonia in 2017. Colonel Wallace would like to thank the NATO CCD COE Director, Merle Maigre, the Law Branch Chief, Lauri Aasmann, and all members of the Law Branch for their collegial assistance and support during the fellowship.

** Lieutenant Colonel Jacobs is an Assistant Professor in the Department of Law, United States Military Academy. The opinions, conclusions, and recommendations in this Article do not necessarily reflect the views of the United States Military Academy, the United States Army or the NATO CCD COE.

TABLE OF CONTENTS

1. INTRODUCTION

Today, we live in a highly computerized, networked world[1] in which the speed, interconnectedness, and sheer volume of computer interactions is growing at an exponential rate.[2] States, industries, and individuals are becoming ever more dependent on information technology and its applications and connections. One need only consider the so-called Internet of Things ("IoT") to put this growth trajectory into perspective. The IoT posits that one day any device with an "on-and-off" switch will be capable of being connected to the Internet. It is estimated by 2020 there will be over twenty-six billion devices connected to the Internet.[3]

When experts at the U.S. Department of Defense Advanced Research Projects Agency ("DARPA")[4] first created the precursor to today's Internet in 1969, it was not possible to predict the broad social, political, and economic ramifications that would be directly attributable to this new technology.[5] What began as a medium for

---

[1] *See* GEORG KERSCHISCHNIG, CYBERTHREATS AND INTERNATIONAL LAW 5 (2012) (describing the depth of global technological interconnectedness).

[2] *See* BRANDON VALERIANO & RYAN C. MANESS, CYBER WAR VERSUS CYBER REALITIES: CYBER CONFLICT IN THE INTERNATIONAL SYSTEM 20 (2015) (conveying the fragility and vulnerability of a system reliant on digital technology).

[3] *See* Jacob Morgan, *A Simple Explanation of 'The Internet of Things'*, FORBES (May 13, 2014), https://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#2543d2761d09 [https://perma.cc/XKV8-QZLL] (highlighting the almost endless number of devices that could be connected to the Internet).

[4] *See About DARPA*, DARPA, https://www.darpa.mil/about-us/about-darpa [https://perma.cc/8XPU-PPXQ] (noting that the mission of DARPA is to make critical investments in technologies for national security and the armed forces). DARPA was formed during the Cold War, in part, out of a sense of national fear and urgency because of technological advancements being made by the Soviet Union. The Internet is but one of DARPA's game-changing technological innovations. Others include: precision weapons and stealth technology, automated voice recognition and language translation, and Global Positioning System receivers small enough to embed in consumer devices.

[5] *See generally* DEP'T OF DEF., THE DEPARTMENT OF DEFENSE CYBER STRATEGY (2015), https://www.defense.gov/Portals/1/features/2015/1415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf [https://perma.cc/RYA5-RAUK] [hereinafter DOD CYBER STRATEGY] (discussing

scientists to quickly and easily share their research grew into an interconnected system of computers and databases linking people all over the world.[6] Experts estimated that, "[b]y the end of 2018 . . . 51.2 percent of the global population . . . will be using the Internet."[7] Moreover, Internet access has increased by over two billion people worldwide during the last decade alone.[8] Food, water, and much of society's critical infrastructure are tied to computer networks, as are transportation, health care, and financial services.[9] Unsurprisingly, this technology of mass empowerment that offers the brightest hope and promise to humankind also produces the greatest concern for peace, stability, and security.[10] Sounding the alarm bell, then-U.S. Secretary of Defense, Leon E. Panetta, in a speech at the Intrepid Sea, Air and Space Museum in New York, issued a dire warning that the United States was facing the possibility of a "cyber-Pearl Harbor" and was increasingly vulnerable to foreign computer hackers. He specifically commented:

> An aggressor nation or extremist group could use these kinds of cyber tools to gain control of critical switches . . . . They could derail passenger trains, or even more dangerous, derail passenger trains loaded with lethal chemicals. They could contaminate the water supply in major cities, or shut down the power grid across large parts of the country.[11]

---

the wide-ranging influence of the Internet on today's social, political and economic landscape).

6 *See generally id.*

7 *New ITU statistics show more than half the world is now using the Internet*, ITU News (Dec. 6, 2018), https://news.itu.int/itu-statistics-leaving-no-one-offline/ [https://perma.cc/9FV9-RR9X].

8 DEP'T OF DEF., *supra* note 5, at 1.

9 *See* NAT'L RES. COUNCIL OF THE NAT'L ACADS., TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 9 (William A. Owens, Kenneth W. Dam & Herbert S. Lin eds., 2009) (conveying the extent to which essential services to society are dependent on the Internet).

10 *See* BENJAMIN WITTES & GABRIELLA BLUM, THE FUTURE OF VIOLENCE: ROBOTS AND GERMS, HACKERS AND DRONES: CONFRONTING A NEW AGE OF THREAT 20 (2015) (acknowledging both the incredible benefits and incredible risks associated with reliance on the Internet across sectors).

11 Elisabeth Bumiller & Thom Shanker, *Panetta Warns of Dire Threat of Cyberattack on U.S.*, N.Y. TIMES (Oct. 11, 2012),

Former Secretary Panetta, as well as many others, highlight the important truth that technology, more than any other outside force, shapes and defines current and future warfare.[12] Of course, this is not new. Technology and military operations have always, to one degree or another, been inextricably linked.[13] From the use of the longbow to machine guns to laser-guided munitions and drones, technological innovations often determine outcomes in war.[14] With respect to current and future warfare, it is nearly impossible to overstate the importance of information technology. Today's armed forces use a range of weapons and munitions that are operated by information technology. The command and control of military forces is increasingly coordinated and directed through computer-based networks that allow common pictures and battlefield analytics to be seen and shared. Logistics are entirely dependent on information systems. And, of course, there are highly sophisticated cyber weapons that can attack an adversary in both virtual and real domains.[15]

In recent years, there has been an exponential growth in the development of both offensive and defensive cyber capabilities across the world. In many respects, cyber conflict has moved to the forefront of many national agendas.[16] Experts estimate that

---

http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html [https://perma.cc/3FPS-NDVZ].

12 *See* Alex Roland, *War and Technology*, FOREIGN POL'Y RES. INST., (Feb. 27, 2009), https://www.fpri.org/article/2009/02/war-and-technology/ [https://perma.cc/3RGD-FV5K] (articulating the impact of technology on global warfare).

13 *See generally* BINARY BULLETS: THE ETHICS OF CYBERWARFARE 1 (Fritz Allhoff, Adam Henschke & Bradley Jay Strawser eds., 2016) (exploring the significant integration of technology into military frameworks worldwide).

14 *See* Michael Marshall, *Timeline: Weapons technology*, NEW SCIENTIST (July 7, 2009), https://www.newscientist.com/article/dn17423-timeline-weapons-technology/ [https://perma.cc/JB7K-JHJW] (discussing the evolution of weapons in light of technological advances).

15 *See* NAT'L RES. COUNCIL OF THE NAT'L ACADS., *supra* note 9, at 9 (examining the capacity of cyber weapons to exploit vulnerabilities and exact damage in both the physical and virtual realm).

16 *See* Gavin Alcott, *Cyberwarfare: Policy Challenges for 21st Century Threats*, PENN WHARTON PUB. POL'Y INITIATIVE (Dec. 6, 2016), https://publicpolicy.wharton.upenn.edu/live/news/1607-cyberwarfare-policy-challenges-for-21st-century [https://perma.cc/G9TC-MM8K] (assessing

approximately 140 countries have developed, or are developing, a capability to wage cyber war.[17] Some countries, like the United States, have established major military organizations focused on cyberspace and operations.[18] In addition to organizational changes, there have also been significant doctrinal changes. For example, in 2016, NATO recognized cyberspace as a domain of operations in which the Alliance must defend itself as effectively as it does in the air, on land, and at sea.[19] Even with the dizzying pace of technological change and innovation, it is important to note that the current legal paradigm regulating conventional warfare (i.e., jus in bello and jus ad bellum) also applies to cyberspace operations.[20] The relationship between these two branches of international law has

---

infrastructural vulnerabilities in the U.S. public and private sectors and identifying policy gaps in the U.S. approach to cyber warfare).

17 *See* Kevin Coleman, *Coleman: The Cyber Arms Race Has Begun*, CSO (Jan. 28, 2008), http://www.csoonline.com/article/2122353/critical-infrastructure/coleman--the-cyber-arms-race-has-begun.html [https://perma.cc/3K8N-4EYC] (evaluating the threats and offensive capabilities developing from the cyber arms race).

18 *See Mission and Vision*, U.S. CYBER COMMAND, https://www.cybercom.mil/About/Mission-and-Vision/ [https://perma.cc/QAF3-8LJY] (noting that the mission of U.S. Cyber Command is "to direct, synchronize, and coordinate cyberspace planning and operations to defend and advance national interests in collaboration with domestic and international partners.").

19 *See* Tomáš Minárik, *NATO Recognises Cyberspace as a 'Domain of Operations' at Warsaw Summit*, CCDCOE (July 21, 2016), https://ccdcoe.org/nato-recognises-cyberspace-domain-operations-warsaw-summit.html [https://perma.cc/6NX4-XHZ6] (discussing the idea of treating cyberspace as a "domain of operations"). *See also* David Alexander, *Pentagon to treat cyberspace as "operational domain"*, REUTERS (July 14, 2011), https://www.reuters.com/article/us-usa-defense-cybersecurity-idUSTRE76D5FA20110714 [https://perma.cc/6NX4-XHZ6] (illustrating the United States' decision to consider cyberspace one of the operational domains in addition to land, air, sea).

20 *See* TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 3 (Michael N. Schmitt gen. ed., 2017) [hereinafter TALLINN MANUAL 2.0] (highlighting that *jus ad bellum* is focused on when a State may use force under international law, but that some commentators have observed that the United Nations Charter has created a legal regime that would more accurately be characterized as *jus contra bellum* because it is fundamentally devised to prevent the use of force). *See also* ROBERT KOLB & RICHARD HYDE, AN INTRODUCTION TO THE INTERNATIONAL LAW OF ARMED CONFLICTS 13 (2010) (elaborating on the relationship between public international law and the law of armed conflict).

been controversial at times. Although a detailed discussion of that relationship is beyond the scope of this Article, it is worth noting that jus in bello and jus ad bellum are distinct in purpose and application and should not be conflated.[21]

This Article addresses issues related to jus in bello, also referred to as international humanitarian law ("IHL").[22] Experts have widely accepted that IHL[23] applies to cyber operations undertaken in the context of an armed conflict.[24] Stated differently, cyber operations in the context of an armed conflict are regulated by well-established norms of IHL. Therefore, the challenge lies not in determining whether the law applies, but rather in determining how, specifically, the law applies to cyber operations. Digital means and methods of warfare executed in both the virtual and real world pose novel issues with respect to IHL. One of the most complex questions that permeates IHL today is how to identify, analyze, and categorize armed conflicts under the current binary conflict classification paradigm established by the 1949 Geneva Conventions when such conflicts include or are limited to cyber operations.

Under IHL, the classification of an armed conflict is the first step in determining the rights and obligations incumbent on the parties to that conflict. IHL recognizes two types of armed conflicts: international and non-international. In an international armed

---

[21] *See generally* Protocol Additional to the Geneva Conventions of 12 Aug. 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), June 8, 1977, 1125 U.N.T.S. 3 [hereinafter AP I] (noting in the preamble that the application of the Protocol must be fully applied without any adverse distinction based on the nature or origin of the armed conflict or on the causes espoused by or attributed to the parties to the conflict).

[22] International humanitarian law is also referred to as either the law of armed conflict or the law of war.

[23] *See* GARY D. SOLIS, THE LAW OF ARMED CONFLICT: INTERNATIONAL HUMANITARIAN LAW IN WAR 21–23 (2016) (discussing the wide acceptance of IHL's application to cyber operations during armed conflict).

[24] *See* TALLINN MANUAL 2.0, *supra* note 20, at 375 (demonstrating that when one thinks of the use of cyber in the context of an armed conflict, it not only involves the employment of cyber capabilities to objectives in and through cyberspace, but also involves weapons reviews to ensure that cyber means of warfare comply with the law of armed conflict).

conflict, the full corpus of IHL applies.[25] By contrast, in a non-international armed conflict, a more limited portion of IHL applies.[26] Finally, in other situations of violence not amounting to an armed conflict, such as sporadic violence, riots, or crime, IHL simply does not apply. However, it is important to note: just because IHL does not apply to a situation of violence does not suggest that there is an international legal normative void. International and regional human rights law, as well as the peacetime domestic law of the State, still applies in those cases.[27]

In discussing the importance of conflict classification under IHL, Professor Michael Schmitt stated:

> Few international humanitarian law topics are proving as problematic in modern warfare as 'classification of conflict', that is, the identification of the type of conflict to which particular hostilities amount as a matter of law. Classifying the conflict in question is always the first step in any international humanitarian law analysis, for the nature of the conflict determines the applicable legal regime. Accordingly, classification is a subject of seminal importance.[28]

The legal and operational complexities associated with conflict classification that include or are limited to cyber operations are multi-faceted. The 2017 *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* addresses the question of conflict

---

[25] *See* GEOFFREY S. CORN ET AL., THE LAW OF ARMED CONFLICT: AN OPERATIONAL APPROACH 71 (2012) (illustrating the application of IHL to both international and non-international conflicts).

[26] *See* JEAN-MARIE HENCKAERTS & LOUISE DOSWALD-BECK, CUSTOMARY INTERNATIONAL HUMANITARIAN LAW: VOLUME I: RULES XXXIV (2005) (suggesting that the amount of substantive IHL protections that apply to a non-international armed conflict is not entirely clear; little codified law applies through common Article 3, Additional Protocol II, and several other IHL treaties, but as a matter of customary law, some influential thought leaders contend that the majority of the substantive rules that apply to an international armed conflict also apply to a non-international armed conflict).

[27] *See* MARCO SASSÒLI, ANTOINE A. BOUVIER & ANNE QUINTIN, HOW DOES LAW PROTECT IN WAR? 124 (2011) (noting that peacetime legal regimes likely provide greater protections with respect to the use of force and detention than IHL).

[28] Michael N. Schmitt, *Classification of Cyber Conflict*, 17 J. CONFLICT & SEC. L. 245 (2012).

classification under IHL in international and non-international armed conflicts that include cyber-threat components. In its nearly 600 pages, the manual also addresses several other vital issues spanning public international law. For context, in 2009, the NATO Cooperative Cyber Defence Centre of Excellence ("NATO CCD COE"), a renowned cyber research and training institution in Tallinn, Estonia,[29] invited a group of independent experts to produce a manual on the international law governing cyber warfare—a manual now known as the *Tallinn Manual 2.0*.[30] This international group of experts, including distinguished scholars and practitioners of international law, examined established legal norms and the applicability of those norms to cyber warfare.[31] In 2013, the *Tallinn Manual on International Law Applicable to Cyber Warfare* was published and released. As a result of the success of the first *Tallinn Manual*, the NATO CCD COE initiated a follow-on project to update the manual and expand its scope to include the international law governing cyber activities during peacetime. This was also done, in part, to respond to the evolving realities of threats and conflict in the cyber realm: on a daily basis, States were wrestling with cyber issues occurring below the threshold sufficient to constitute a use of force. In fact, those events were far more prevalent than issues related to the use of force or the conduct of hostilities, which were the domain of the first *Tallinn Manual*.[32]

---

[29] *See generally About Cyber Defence Centre*, CCDCOE, https://ccdcoe.org/about-us.html [https://perma.cc/89CJ-2N4M] (discussing that the mission of the NATO Cooperative Cyber Defence Centre of Excellence is to enhance the capability, cooperation and information sharing among NATO, NATO nations and partners in cyber defense through education, research and development, lessons learned and consultation).

[30] *See generally* TALLINN MANUAL 2.0, *supra* note 20.

[31] *See generally id.*

[32] Impressively, *Tallinn Manual 2.0* contains 154 rules, including two specific rules on international and non-international armed conflict, Rules 82 and 83. The detailed commentary accompanying each rule not only offers important insights into the deliberations and thought processes of the experts regarding the legal basis and justification for the rules and their normative context, but also offers practical implications of the rules' application in a cyber context. This level of detail is particularly helpful for national legal advisors and academics. Additionally, the commentaries to the rules express the positions articulated by the experts in their internal discussions so that it is evident to the reader whether the Experts were able to reach a consensus on a particular issue. Finally, and most importantly, it is

2. CYBER OPERATIONS CASE STUDIES

Armed conflicts that include or are limited to cyber operations can be challenging to classify within the IHL legal framework. In fact, some of the most well-known, highly publicized cyber incidents fail to meet the threshold for either international or non-international armed conflict under IHL. That is not to say that such incidents occur in an international normative gap; they do not. Rather, such incidents are regulated by legal regimes, whether domestic or international, which otherwise operate during peacetime. Such legal regimes possess their own distinct frameworks of rights, duties, processes, and potential sanctions. The case studies outlined below highlight how four unique situations of violence involving cyber operations are either international or non-international armed conflicts subject to IHL regulation or how they are neither.

The first case study involving Estonia is a situation not amounting to an armed conflict. On April 27, 2007, Estonia was hit by a large-scale, persistent series of distributed denial of service ("DDoS")[33] attacks. These attacks overwhelmed and shut down the websites of Estonian government ministries, political parties, newspapers, banks, and companies.[34] The attacks were particularly harmful in Estonia—given its reliance on the Internet for everything from grocery shopping and parking, to banking and voting. The DDoS cyber-attacks were part of a larger protest movement[35] following a highly-controversial decision by the Estonian government to relocate a Soviet war memorial from its original

---

important to understand and appreciate that the experts were limiting themselves to an objective restatement of the *lex lata*. They avoided including statements reflecting the *lex ferenda*. *See id.* at 3 (highlighting the approach of the authors regarding the concept of *lex lata*).

[33] *See id.* at 564–65 (noting that DDoS is a method that employs many different computing devices to cause a denial of service to single or multiple targets).

[34] *See* HEATHER HARRISON DINNISS, CYBER WARFARE AND THE LAWS OF WAR 38–39 (2014) (highlighting the attacks' effects on Estonian websites).

[35] *See* Steven Lee Myers, *Estonia removes Soviet-era war memorial after a night of violence*, N.Y. TIMES (Apr. 27, 2007), http://www.nytimes.com/2007/04/27/world/europe/27iht-estonia.4.5477141.html [https://perma.cc/CR6F-N33V] (discussing the removal of a Soviet-era war memorial and resulting protests and violence).

location in the center of Tallinn to a military cemetery on the outskirts of the city. The Soviets originally built the monument in 1947 to commemorate their war dead after defeating the Nazis in the Baltic region.[36] The culprits of the cyber-attacks were believed to be a small group of Russian activists associated with the pro-Kremlin youth group, Nashi.[37] These attacks appeared to come from Russian IP addresses with online instructions written in Russian. Furthermore, Russia ignored the Estonian government's appeals for assistance.[38]

The second case study involves the armed conflict between Russia and Georgia in the summer of 2008—an effort to exert control over an ethnic enclave bordering the two countries known as South Ossetia. In 1990, South Ossetia had declared its independence from Georgia and, following "a two-year war and an imperfect ceasefire . . . operated for nearly two decades as [an] independent state."[39] In 2008, Georgia launched a military offensive to retake control of South Ossetia.[40] Russia, which had long supported South Ossetia's secessionist efforts, sent its armed forces into South Ossetia and also targeted important military and transport hubs situated elsewhere within Georgia.[41] Georgia's defenses were wholly

---

[36] *See* Joshua Davis, *Hackers Take Down the Most Wired Country in Europe*, WIRED (Aug. 21, 2007), https://www.wired.com/2007/08/ff-estonia/ [https://perma.cc/W9N9-7XEW] (providing background information on a war memorial and the consequences facing the Estonian government for removing it).

[37] *See* Christian Lowe, *Kremlin loyalist says launched Estonia cyber-attack*, REUTERS (Mar. 13, 2009), https://www.reuters.com/article/us-russia-estonia-cyberspace/kremlin-loyalist-says-launched-estonia-cyber-attack-idUSTRE52B4D820090313 [https://perma.cc/9HU7-TEXS] (examining a pro-Kremlin youth activist's claim that the organization was behind the electronic attack on Estonia).

[38] *See* Damien McGuinness, *How a cyber attack transformed Estonia*, BBC (Apr. 27, 2017), http://www.bbc.com/news/39655415 [https://perma.cc/PX85-SNP6] (noting the Russian government's limited involvement in the Estonian conflict).

[39] Stephanie Joyce, *Along A Shifting Border, Georgia And Russia Maintain An Uneasy Peace*, NPR (Mar. 13, 2017), http://www.npr.org/sections/parallels/2017/03/13/519471110/along-a-shifting-border-georgia-and-russia-maintain-an-uneasy-peace [https://perma.cc/GF4J-5Z3W].

[40] *See id.* (explaining that, in August 2008, "Georgia launched an offensive of the breakaway region.").

[41] *See* Charles King, *The Five-Day War: Managing Moscow After the Georgia Crisis*, FOREIGN AFFAIRS (Nov.-Dec., 2008),

inadequate to rebuff Russia's aggressions, and the ensuing five-day armed conflict killed hundreds of people and sent thousands of refugees to temporary shelters.[42] In addition to the kinetic fight, Russia launched cyber operations against Georgia both before and during the international armed conflict. In so doing, Russia demonstrated the effectiveness of cyber operations in support of a conventional conflict.[43] In particular, a number of Georgian government websites were defaced and had their content replaced with anti-Georgian messages.[44] In fact, the multiple D.D.O.S. attacks resulted in the website of the Georgian president being inoperable for 24 hours.[45] The cyber-attack, overall, severely limited Georgia's ability to disseminate information.[46] At the operational and tactical levels, it is believed that Russian cyber operations were closely coordinated with conventional forces to enhance operational effectiveness. For example, "networks and web sites within specific geographic locations were targeted for denial and disruption operations in order to cause panic and uncertainty (disruption) in the Georgian civilian population."[47] As noted by David Hollis, Russia's use of cyber operations against Georgia "appears to be the first case in history of a coordinated cyberspace domain attack synchronized with major combat actions in the other warfighting domains (consisting of Land, Air, Sea, and Space)."[48]

---

https://www.foreignaffairs.com/articles/russia-fsu/2008-11-01/five-day-war [https://perma.cc/KY8B-K9AK] (discussing the response of Georgian forces to attacks by secessionists in South Ossetia).

42 *See id.* (describing the consequences of the attacks by secessionists in South Ossetia).

43 *See* DINNISS, *supra* note 34, at 8 (explaining Russia's approach to its conflict with Georgia).

44 MARCO ROSCINI, CYBER OPERATIONS AND THE USE OF FORCE IN INTERNATIONAL LAW 8 (2016) (describing the positive effects of cyber operations in Russia).

45 John Markoff, *Before the Gunfire, Cyberattacks*, N.Y. TIMES (Aug. 12, 2008), http://www.nytimes.com/2008/08/13/technology/13cyber.html (noting the effects of the cyberspace attack on Georgia).

46 *Id.*

47 David Hollis, *Cyberwar Case Study: Georgia 2008*, SMALL WARS JOURNAL (Jan. 6, 2011), https://smallwarsjournal.com/blog/journal/docs-temp/639-hollis.pdf [https://perma.cc/VG99-JTES].

48 *Id. See also generally* PAUL ROSENZWEIG, CYBER WARFARE: HOW CONFLICTS IN CYBERSPACE ARE CHALLENGING AMERICA AND CHANGING THE WORLD 33 (2013) (detailing the Russian–Georgian war).

The third case study is *Operation Olympic Games*, a highly sophisticated and targeted cyber-attack, reportedly launched (but never officially acknowledged) by the United States and Israel against an Iranian nuclear enrichment facility at Natanz, Iran. Fred Kaplan's book, *Dark Territory: The Secret History of Cyber War*, details the events leading up to the operation beginning in 2006. According to Kaplan, President Bush wanted to derail or slow down the Iranian nuclear program. President Bush did not, however, want to launch airstrikes against the Iranian nuclear enrichment facility. Instead, he sought an option between doing nothing and a kinetic attack. President Bush settled on a cyber-attack on the computer control systems at the Natanz facility.[49] After creating and covertly inserting a cyber "beacon" into the Iranian computer network to map out the workings of the plant, attackers inserted a highly complex worm, sometimes called "Stuxnet,"[50] into the plant's computer controller system.[51] The Stuxnet worm took over some of the uranium enrichment centrifuges operated by the control system, making them spin either too fast or too slow.[52] This process made them unbalanced and, in some cases, caused centrifuges to explode. Over time, new variants of the Stuxnet worm were created and surreptitiously inserted into the control systems resulting in slightly different failures.[53] Stuxnet was designed to leave no trace of the

---

[49] *See generally* FRED KAPLAN, DARK TERRITORY: THE SECRET HISTORY OF CYBER WAR 203–4 (2016) (describing the American government's response to *Operation Olympic Games*).

[50] *See* Kim Zetter, *An Unprecedented Look at Stuxnet, the World's First Digital Weapon*, WIRED (Nov. 3, 2014), https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/ [https://perma.cc/95UT-84HS](discussing the discovery of the Stuxnet by a Belarus security firm hired to troubleshoot a series of computers in Iran that were malfunctioning).

[51] Guilbert Gates, *How a Secret Cyberwar Program Worked*, N.Y. TIMES (June 1, 2012), http://www.nytimes.com/interactive/2012/06/01/world/middleeast/how-a-secret-cyberwar-program-worked.html [https://perma.cc/TP4Y-DZU6] (describing the way secret cyberwar programs work).

[52] *See Uranium Enrichment*, U.S. NRC (Aug. 2, 2017), https://www.nrc.gov/materials/fuel-cycle-fac/ur-enrichment.html [https://perma.cc/3CFB-XXM4] (describing the process of uranium enrichment).

[53] See Gates, *supra* note 51 (discussing the changes made to Stuxnet and the resulting consequences of those changes).

attackers.[54] General Michael Hayden, the former director of the NSA and CIA, commented on this milestone in modern warfare:

> Previous cyber-attacks had effects limited to other computers . . . This is the first attack of a major nature in which a cyber-attack was used to effect physical destruction. And no matter what you think of the effects--and I think destroying a cascade of Iranian centrifuges is an unalloyed good--you can't help but describe it as an attack on critical infrastructure . . . .Somebody has crossed the Rubicon. We've got a legion on the other side of the river now. Something had shifted in the nature and calculation of warfare, just as it had after the United States dropped atom bombs on Hiroshima and Nagaskai at the end of World War II.[55]

The last case study involves the United States' fight against the Islamic State of Iraq and Syria ("ISIS"). In addition to conventional and special operations combat against ISIS fighters in Iraq, Syria, and elsewhere, the United States launched a new cyber campaign against ISIS forces in 2016.[56] Such a response to ISIS is appropriate and necessary, in part, because no other non-State armed group in history has capitalized more on information technology. ISIS has demonstrated that it is extremely adept at using this technology for such functions as command and control of its forces, recruitment, and propaganda, among other things.[57] One particular operation against ISIS, code-named *Operation Glowing Symphony*, was carried

---

[54] Paul Szoldra, *A new film gives a frightening look at how the US used cyberwarfare to destroy nukes*, BUS. INSIDER (Jul. 7, 2016), http://www.businessinsider.com/zero-days-stuxnet-cyber-weapon-2016–7 [https://perma.cc/XP3V-HAFG] (discussing the effects of Stuxnet). *But see* David E. Sanger, *Obama Order Sped Up Wave of Cyberattacks Against Iran*, N.Y. TIMES (June 1, 2012), http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html [https://perma.cc/6U4T-DFUQ] (describing a programming error that caused an element of the program to become public).

[55] KAPLAN, *supra* note 49, at 215.

[56] David E. Sanger, *U.S. Cyberattacks Target ISIS in a New Line of Combat*, N.Y. TIMES (Apr. 24, 2016), https://www.nytimes.com/2016/04/25/us/politics/us-directs-cyberweapons-at-isis-for-first-time.html [https://perma.cc/U5ED-6JK8] (discussing how the United States directed cyber weapons at ISIS).

[57] *See id.* (discussing ISIS's proficient use of technology).

out by U.S. Cyber Command's Joint Task Force Ares.[58] As part of the operation, Task Force Ares removed ISIS propaganda and locked ISIS administrators out of their accounts. A debate arose, however, surrounding whether the U.S. must disclose its plan to conduct cyber operations to countries whose servers may house ISIS data, outside of the battlefields of Syria and Iraq.[59] One significant impact that has been attributed, at least in part, to cyber operations against ISIS is the reduction in the number of foreign fighters going to Mideast conflict zones to join ISIS—new recruits have dropped from 2,000 per month to 500, and overall personnel strength has dropped from 35,000 to 20,000.[60]

These four case studies on cyber operations illustrate the spectrum of conflict in the cyber realm. Depending upon where the situation falls along the spectrum, IHL either does not apply at all, applies minimally, or applies fully. Without question, some cases are more difficult to assess than others, as will be seen in the analysis below. Implicit in any analysis of conflict classification is the fact that there must be some nexus between the cyber operation or activity and the conflict for IHL to apply. In other words, if a cyber activity occurs but is unrelated to the armed conflict, IHL does not regulate it. Not surprisingly, there can be significant debate as to the nature and scope of that nexus.[61] Beyond that threshold connection, looking at conflict classification under IHL through a cyber lens raises many challenging issues.

---

[58] Ellen Nakashima, *U.S. military cyber operation to attack ISIS last year sparked heated debate over alerting allies*, WASH. POST (May 9, 2017), https://www.washingtonpost.com/world/national-security/us-military-cyber-operation-to-attack-isis-last-year-sparked-heated-debate-over-alerting-allies/2017/05/08/93a120a2-30d5-11e7-9dec-764dc781686f_story.html?utm_term=.6cc9d75e8b91 [https://perma.cc/9SGU-86C3] (explaining how the U.S. government conducted *Operation Glowing* Symphony).

[59] *See id.*

[60] Rowan Scarborough, *Obama launches first cyberwar against isis, cuts recruiting by 75 percent*, WASH. TIMES (Sept. 12, 2016), http://www.washingtontimes.com/news/2016/sep/12/obama-administration-takes-isis-fight-into-cybersp/ [https://perma.cc/JR9W-K9X2] (asserting a relationship between the Obama administration's first cyberwar and a reduction in the number of foreign fighters joining the terrorist army in Syria).

[61] *See* TALLINN MANUAL 2.0, *supra* note 20, at 376 (discussing the relationship between IHL and cyber conflicts).

3. CONFLICT CLASSIFICATION UNDER INTERNATIONAL HUMANITARIAN LAW—AN OVERVIEW

For the period following the Peace of Westphalia up until the end of World War II, the jus in bello applied almost exclusively to wars between States.[62] Unpacking this historical context, Professor Akande observed:

> This was a consequence of the fact that international law as a whole was concerned only with relations between States and eschewed regulations of matters considered to be within the domestic jurisdiction of States. Internal armed conflicts, or civil wars, were not considered to be 'real war[s] in the strict sense of the term in International Law,' since that term was reserved for conflicts between States.[63]

IHL applied to internal armed conflicts only under very limited circumstances, in which either the State involved or a third State recognized the belligerency of the insurgent group.[64] Recognition of belligerency was permitted—thereby triggering IHL—if the insurgent group: (1) occupied territory; (2) established a government which exercised sovereign rights over the territory it occupied; and (3) complied with the laws and customs of war during hostilities with the State.[65] In the aftermath of World War II, there were seismic changes to IHL generally and conflict classification specifically.

On August 12, 1949, a diplomatic conference in Geneva, Switzerland approved the text of four conventions—the 1949 Geneva Conventions—which more States have ratified than any

---

62 *See* Dapo Akande, *Classification of Armed Conflicts: Relevant Legal Concepts, in* 32 INTERNATIONAL LAW AND THE CLASSIFICATION OF CONFLICTS 33 (Elizabeth Wilmshurst ed., 2012) (discussing the classification of conflict type during the specified time period).

63 *Id.*

64 *See id.* (discussing the growing application of IHL to intra-State warfare in the years leading up to World War II, particularly during the and Spanish Civil War).

65 Dietrich Schindler, *Non-International Armed Conflicts*, *in* THE SCOPE AND APPLICABILITY OF INTERNATIONAL HUMANITARIAN LAW 48 (Michael N. Schmitt & Wolff Heintschel von Heinegg eds., 2012) (citation omitted).

other international agreements in the laws regulating warfare.[66] The Conventions were, in part, borne out of the unprecedented violence and suffering of World War II.[67] As Ambassador George H. Aldrich commented:

> [T]he 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.[68]

---

[66] *See* ADAM ROBERTS & RICHARD GUELFF, DOCUMENTS ON THE LAWS OF WAR 195 (2000) (describing the four 1949 Geneva Conventions). To provide some background and context, the Geneva Conventions can be traced back to a well-to-do Swiss businessman, Henry Dunant, and the Battle of Solferino in 1859. The Battle of Solferino in Lombardy, not far from Milan and Verona, was fought between the forces of Austria and a French-Piedmontese alliance. The battle was one of the bloodiest of the 19th century with thousands of dead and wounded on both sides. The military practice of the time was to leave the wounded where they had fallen on the battlefield. Dunant witnessed the carnage. After the battle, he provided aid and comfort to survivors. Dunant could not forget what he saw and experienced. In 1862, he published a small book entitled *A Memory of Solferino*. In the book, Dunant vividly and graphically described the battle and the suffering of the wounded soldiers. He also called for the creation of relief societies in each country that would act as auxiliaries to the army medical services and facilitate care for all wounded and sick, regardless of State affiliation. This effort led eventually to the formation of the International Committee of the Red Cross. 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. 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. 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." *See Solferino and the International Committee of the Red Cross*, INT'L COMM. RED CROSS (June 1, 2010), https://www.icrc.org/eng/resources/documents/feature/2010/solferino-feature-240609.htm [https://perma.cc/5T44-4DWN] (discussing Dunant's contributions to Red Cross and Geneva Conventions).

[67] *See* Philip Spoerri, Director of Int'l Law, Int'l Comm. Red Cross, Address at the Ceremony to Celebrate the 60th Anniversary of the Geneva Conventions (Dec. 8, 2009), https://www.icrc.org/eng/resources/documents/statement/geneva-conventions-statement-120809.htm [https://perma.cc/L36W-5SZP] (discussing the origins of the Geneva Conventions).

[68] SOLIS, *supra* note 23, at 88.

Generally speaking, the 1949 Conventions expanded the scope of IHL to include the addition of a fourth convention that focused on the protection of civilians during armed conflicts.[69] Additionally, the other three Conventions were updated and revised.[70] Among the revisions was the creation of two articles that are included, in identical form, in all four of the Geneva Conventions – Common Articles 2 and 3. More influential than other treaties, the four 1949 Geneva Conventions are the cornerstone of modern IHL.[71]

Of the many important contributions made by the 1949 Geneva Conventions to the corpus of IHL, perhaps none is of greater consequence than the binary conflict classification paradigm prescribed by common Articles 2 and 3.[72] This new legal classification framework marked a sea change in the conceptualization of wars. As mentioned previously, the jus in bello was developed in the context of wars between States, applying only to conflicts of an international nature with little application to civil wars.[73] Moreover, the Geneva Conventions of 1864, 1906, and 1929 did not have a specific provision defining the scope of their application.[74] It was not until the 1949 Geneva Conventions that a

---

[69] *See* Geneva Convention Relative to the Protection of Civilian Persons in Time of War, Aug. 12, 1949, ar. 3, 6 U.S.T. 3516, 75 U.N.T.S. 287.

[70] *See* CORN ET AL., *supra* note 25, at 70 (describing the four Geneva Conventions).

[71] *See* SOLIS, *supra* note 23, at 88 (describing the Geneva Conventions). Historically, the *jus in bello* was perceived to have two traditions or families: "Hague Law" and "Geneva Law." The primary focus of Hague Law was to regulate the conduct of hostilities. By contrast, Geneva Law focused on the protections of the victims of armed conflict. Today, those distinctions do not exist. IHL is an amalgamation of both Hague and Geneva Law. *Id.*

[72] *See Id.* at 91 (describing the Conventions' articles). As the name implies, common articles are contained in all four Geneva Conventions. That is, the substance of the articles is so important that the drafters of the Conventions included the same or similar articles in each of the four Conventions. In a sense, the common articles, along with certain general principles, link the four Conventions. The common articles, of which there are about twenty, are found among the general provisions at the beginning of each Convention, among the articles relating to treaty execution, and among the concluding procedural provisions. *See also* ROBERTS & GUELFF, *supra* note 66, at 195 (discussing the common articles among the Geneva Conventions).

[73] *See* Akande, *supra* note 62, at 33 (discussing conflict classification).

[74] *See* INT'L COMM. RED CROSS, COMMENTARY OF 2016, art. 2, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Comment.xsp?action=openDocument&doc

distinction between international armed conflicts and non-international armed conflicts was codified.

The scope and applicability of IHL depends on the existence of an armed conflict.[75] This is true for both international and non-international armed conflicts because IHL did not adopt a unitary concept of an armed conflict.[76] Interestingly, even though the notion of an armed conflict is perhaps the single most important concept in IHL, it has never been defined by a treaty.[77] Some publicists have even commented that the drafters of the 1949 Geneva Conventions avoided a rigid definition of an armed conflict because such a formulation might limit the applicability of the treaties.[78] To fully understand and appreciate the binary conflict classification paradigm, it is necessary to look at common Articles 2 and 3 separately.

4. COMMON ARTICLE 2: INTERNATIONAL ARMED CONFLICTS

Common Article 2 to the 1949 Geneva Conventions states:

> In addition to the provisions which shall be implemented in peacetime, the present Convention shall apply to all cases of declared war or of any other armed conflict which may arise between two or more of the High Contracting Parties, even if the state of war is not recognized by one of them.
>
> The Convention shall also apply to all cases of partial or total occupation of the territory of a High Contracting Party, even if the said occupation meets with no armed resistance.
>
> Although one of the Powers in conflict may not be a party to the present Convention, the Powers who are parties thereto

---

umentId=BE2D518CF5DE54EAC1257F7D0036B518#_Toc452041590 [hereinafter 2016 COMMENTARY, GC I].

75 *See* KOLB & HYDE, *supra* note 20, at 74 (discussing the application of the laws of armed conflicts).

76 *Id.*

77 *See* WILLIAM H. BOOTHBY, THE LAW OF TARGETING 45 (2012) (discussing various attempts to define armed conflicts).

78 *See* SOLIS, *supra* note 23, at 159 (discussing the implications of defining an armed conflict for IHL purposes).

> shall remain bound by it in their mutual relations. They shall furthermore be bound by the Convention in relation to the said Power, if the latter accepts and applies the provisions thereof.[79]

At its core, this foundational provision establishes the circumstances and conditions under which the four Conventions apply.[80] Specifically, the Conventions, in their entirety, are triggered by a declared war,[81] an international armed conflict, or a partial or total occupation.[82] A fourth situation covering wars of national liberation was added with Article 1(4) of Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts ("Protocol I").[83] This provision "widened the scope of applicability of the law

---

[79] Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in the Armed Forces in the Field art. 2, Aug. 12, 1949, 6 U.S.T. 3114, 75 U.N.T.S. 31 [hereinafter Geneva I].

[80] *See* 2016 COMMENTARY, GC I, *supra* note 74, at para. 192 ("This provision is a central pillar of the Geneva Conventions as it establishes the circumstances and conditions under which the Conventions apply.").

[81] *See id.* at paras. 203–209 (defining declared war).

[82] *See* Geneva I, *supra* note 79, at art. 2. The portion of IHL that addresses a total or partial occupation is embodied in selected provisions of the Annexed Regulations to Hague Convention IV of 1907, the Fourth Geneva Convention of 1949, and customary international law. Accordingly, the entirety of IHL is triggered when a successful invader establishes effective control over enemy territory. That is, a territory is considered occupied once it is placed under the authority of a hostile army.

[83] *See generally* Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I) art.1(4), June 8, 1977, 1125 U.N.T.S. 3 [hereinafter AP I]. Article 1(4), sometimes referred to as the "CARs" provision (*colonial* domination, *alien* occupation, and *racist* regimes), was one of the objectionable points for the United States in terms of ratifying AP I. The provision provided as follows:

> 4. The situations referred to in the preceding paragraph include armed conflicts in which peoples are fighting against colonial domination and alien occupation and against racist régimes in the exercise of their right of self-determination, as enshrined in the Charter of the United Nations and the Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations.

governing international armed conflicts by recognizing so-called 'internationalized' wars, although the kinds of armed conflict that fall into that 'new' category remain unsettled."[84] Thus, if the factual situation meets the criteria for one of the four situations outlined above, it can be said to be an international or inter-State armed conflict.[85] It is important to note that it does not matter whether a party or parties to the armed conflict deny the existence of an armed conflict for political or other reasons. Conflict classification depends only on the circumstances prevailing on the ground at the time.[86] Of course, the key inquiry from an IHL perspective is *when* an armed conflict exists between two or more States such that the body of law is triggered.[87]

To adequately address this question, it is necessary to provide some background and context about several important IHL concepts related to or embedded in common Article 2. First, the general criteria in common Article 2 have crystallized into rules that govern the applicability of *all* IHL rules under international armed conflicts, for both customary and conventional law, and are not limited only to the applicability of the four 1949 Geneva Conventions.[88] Accordingly, all IHL treaties, including older ones, as well as

---

The essence of the objection is that it blurs the distinction between international and non-international armed conflicts based upon the asserted motive of the non-State group fighting against the government of a State. *See* SOLIS, *supra* note 23, at 133 (explaining the U.S. objection to ratifying the Convention).

84 Wolff Heintschel von Heinegg, *Introduction*, *in* THE SCOPE AND APPLICABILITY OF INTERNATIONAL HUMANITARIAN LAW, *supra* note 65, at xi.

85 KOLB & HYDE, *supra* note 20, at 74.

86 2016 COMMENTARY, GC I, *supra* note 74, at para. 211 ("Article 2(1) underlines the pre-eminence of the factual existence of armed conflict over the formal status of war.").

87 *See* Akande, *supra* note 62, at 39 (discussing how to define an armed conflict). Although beyond the scope of this Article, there is also the question of when an international armed conflict ends. Assessing the end of an armed conflict can be a very difficult matter. An international armed conflict ends when there has been a general close of military operations. *See* CORN ET AL., *supra* note 25, at 70 ("The drafters [of Common Articles 2 and 3] responded to the inherent insufficiency of the international definition of war as the trigger for law application, by including law triggering articles in the revised Conventions and the humanitarian protections they provide.").

88 KOLB & HYDE, *supra* note 20, at 75.

customary international law applies to a declared war, an international armed conflict, or a partial or total occupation.[89]

Second, as highlighted previously, common Article 2(1) introduced, but did not define, the term "armed conflict" into the IHL lexicon, making the application of the law less dependent upon the formalisms associated with a declared war.[90] The term "armed conflict" connotes an objective standard to be assessed on the basis of the prevailing facts.[91] As such, from 1949 onwards, the notion of armed conflict supplanted the traditional concept of war under IHL.[92] Because the term "armed conflict" was not defined in the 1949 Geneva Conventions or in any other IHL treaty, Common Article 2 in no way qualifies "the armed conflict" with scope, duration, or intensity requirements.[93] This leaves the interpretation and amplification of the term "armed conflict" in the hands of tribunals and commentators to provide such clarity.

Third, the Appeals Chamber of the International Criminal Tribunal for the former Yugoslavia (ICTY) proposed a definition of international armed conflict in its landmark *Tadić* (Appeal on Jurisdiction) case. The Tribunal stated, in part, as follows:

> [A]n armed conflict exists 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. International humanitarian law applies from the initiation of such armed conflicts and extends beyond the cessation of hostilities until a general conclusion of peace is reached; or, in the case of internal conflicts, a peaceful settlement is achieved. Until that moment, international humanitarian law continues to

---

89 *Id.*

90 *See* 2016 COMMENTARY, GC I, *supra* note 74, at para. 193 ("Article 2(1) broadens the Geneva Conventions' scope of application by introducing the notion of 'armed conflict', thereby making their application less dependent on the formalism attached to the notion of 'declared war'.").

91 *Id.* at para. 211 ("[T]he determination of the existence of an armed conflict within the meaning of Article 2(1) must be based solely on the prevailing facts demonstrating the *de facto* existence of hostilities between the belligerents, even without a declaration of war.").

92 SASSÒLI, BOUVIER & QUINTIN, *supra* note 27, at 122.

93 CORN ET AL., *supra* note 25, at 74.

> apply in the whole territory of the warring States or, in the case of internal conflicts, the whole territory under the control of a party, whether or not actual combat takes place there.[94]

Having established that legal scaffolding, the next task is to determine what "international" and "armed" mean in terms of common Article 2. In this regard, "'[i]nternational' . . . is effectively synonymous with inter-state."[95] The most obvious situation involves two or more States as parties to the conflict on opposing sides.[96] Furthermore, a conflict is internationalized when a non-State armed group—acting under the control of a State party—engages in hostilities against an opposing State party.[97] Again, from the *Tadić* case, the ICTY considered the issue of whether Bosnian Serb units were sufficiently directed by the Federal Republic of Yugoslavia to conclude that an international armed conflict existed for the purposes of conflict classification under IHL.[98] In articulating the overall control standard, the Appeals Chamber stated, in part, as follows:

> [C]ontrol by a State over subordinate armed forces or militias or paramilitary units may be of an overall character (and must comprise more than the mere provision of financial assistance or military equipment or training). This requirement, however, does not go so far as to include the issuing of specific orders by the State, or its direction of each individual operation. Under international law it is by no means necessary that the controlling authorities should plan all the operations of the units dependent on them, choose their targets, or give specific instructions concerning the conduct of military operations and any alleged violations of international humanitarian law. The control required by international law may be deemed to exist when a State (or,

---

94 Prosecutor v. Tadić, Case No. IT-94-1-I, Decision on Defence Motion for Interlocutory Appeal on Jurisdiction, ¶ 70 (Int'l Crim. Trib. for the Former Yugoslavia Oct. 2, 1995).

95 CORN ET AL. *supra* note 25, at 82.

96 TALLINN MANUAL 2.0, *supra* note 20, at 380.

97 *Id.*

98 *Id.*

> in the context of an armed conflict, the Party to the conflict) has a role in organising, coordinating or planning the military actions of the military group, in addition to financing, training and equipping or providing operational support to that group.[99]

Under this standard, the legal threshold is relatively high for internationalizing a conflict that involves subordinate or "proxy" forces. Accordingly, merely providing support to non-State actors does not internationalize it pursuant to common Article 2.[100] Moreover, a non-State armed group, as a collective entity, means something more than just an individual or an insufficiently organized group.[101] Put in a slightly different way, the overall control test is a manifestation of the application of well-established legal principles of the law of State responsibility in determining whether and when non-State armed groups amount to *de facto* agents of a third State.[102] In contrast to the "international" requirement under common Article 2, the "armed" requirement can be even more complex in theory and application.

In *Tadić*, the ICTY set and reinforced a relatively low legal benchmark for the "armed" element of an international armed conflict. The standard the court created is: "whenever there is a resort to armed force between States."[103] As such, there is neither a duration requirement nor an intensity requirement in terms of the number of victims or the destruction of property. Even with this low standard, which is intended to provide the broadest possible IHL coverage, there are some situations that would not trigger an international armed conflict in terms of State practice. For example, the replacing of border patrol agents with members of the armed forces; an accidental incursion into the sovereign territory of another State; or the accidental bombing within the territory of another

---

[99] Prosecutor v. Tadić, Case No. IT-94-1-A, Appeals Chamber Judgment, ¶ 137 (Int'l Crim. Trib. for the Former Yugoslavia July 15, 1999).

[100] TALLINN MANUAL 2.0, *supra* note 20, at 381.

[101] *Id.*

[102] SASSÒLI, BOUVIER & QUINTIN, *supra* note 27, at 122 (explaining the standard rule that "a conflict between governmental forces and rebel forces within a single country becomes of international character if the rebel forces are *de facto* agents of a third State").

[103] Prosecutor v. Tadić, *supra* note 94, at ¶ 70.

country would not, in and of themselves, trigger an international armed conflict under IHL.[104] The 1960 commentary to the Third Geneva Convention succinctly synopsized the intent of States with respect to the low "armed" requirement under common Article 2:

> Any difference arising between two States and leading to the intervention of members of the armed forces is an armed conflict within the meaning of Article 2, even if one of the Parties denies the existence of a state of war. It makes no difference how long the conflict lasts, how much slaughter takes place, or how numerous are the participating forces; it suffices for the armed forces of one Power to have captured adversaries falling within the scope of Article 4. Even if there has been no fighting, the fact that persons covered by the Convention are detained is sufficient for its application. The number of persons captured in such circumstances is, of course, immaterial.[105]

Applying the above to digital operations, *Tallinn Manual 2.0 -- Rule 82* speaks to cyber operations in the context of an international armed conflict. It states: "[a]n international armed conflict exists whenever there are hostilities, which may include or be limited to cyber operations, between two or more States."[106] Two of the above case studies may fairly be characterized as international armed conflicts under Rule 82 and two may not.

The first is the most straightforward and arguably the least controversial, *i.e.*, the international armed conflict between Russia and Georgia in 2008. But, as the analysis below will demonstrate, even the most straightforward incident raises significant legal issues when the conflict includes or is limited to cyber operations. In the Russian-Georgian international armed conflict over South Ossetia, there were cyber operations that occurred before and during the

---

104 BOOTHBY, *supra* note 77, at 45.

105 COMMENTARY, III GENEVA CONVENTION RELATIVE TO THE TREATMENT OF PRISONERS OF WAR 67 (Jean S. Pictet ed., 1960), https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Comment.xsp?action=openDocument&documentId=07B4DAD7719E37E4C12563CD00424D17 [https://perma.cc/7J3P-K5UN] [hereinafter Commentary, GC III].

106 TALLINN MANUAL 2.0, *supra* note 20, at 379.

conventional fighting.[107] The cyber operations launched by Russia against Georgia raise a number of challenging questions. The first question is: when precisely did the international armed conflict commence? The answer to this question is important because the start date is what triggers the application of IHL.[108] As early as July 20, 2008, there were DDoS attacks that shut down Georgian servers.[109] On or about August 8, 2008, Russia conducted airstrikes against Georgian targets and Russian troops physically moved into South Ossetia to provide support to the separatists in their fight against Georgia.[110]

So, did the armed conflict start on August 8th with the conventional attack, or did it begin approximately three weeks earlier with the DDoS attacks? Complicating that answer are two other related, subsidiary questions. The first is the ever-thorny question of attribution. Who precisely authorized and conducted the cyber operations against Georgia: military electronic warriors, patriotic hackers, cyber criminals, or some other groups? In cyberspace, it is easy to cloak identities, operate through third-parties, and route operations through servers from around the world, making it very difficult to attribute the cyber operations to a particular State, group, or individual.[111] Also, with respect to the DDoS attacks beginning on July 20th, was there a sufficient nexus between those cyber-attacks and the conventional armed conflict that began three weeks later? Given the above, even the most uncomplicated scenario is riddled with uncertainty about when the international armed conflict started and who precisely was a party to it. Over and above the other questions, assuming *arguendo*, that the organization that launched the cyber operations against Georgia was either an organ of the Russian State or a *de facto* agent of Russia,

---

107 Hollis, *supra* note 47, at 2–3.

108 *See generally* Markoff, *supra* note 45 (elaborating on the extent of cyber operations conducted against Georgia and when those activities began).

109 *Id.*

110 Michael Schwirtz, Anne Barnard & C. J. Chivers, *Russia and Georgia Clash Over Separatist Region*, N.Y. TIMES (Aug. 9, 2008), http://www.nytimes.com/2008/08/09/world/europe/09georgia.html [https://perma.cc/PC4P-NBFQ].

111 *See, e.g.*, Noah Shachtman, *Top Georgian Official: Moscow Cyber Attacked Us – We Just Can't Prove It*, WIRED (Mar. 11, 2009), https://www.wired.com/2009/03/georgia-blames/ [https://perma.cc/H248-TTBC] (noting the difficulties of pinpointing the sources of cyber operations in the investigation of an attack against Georgian cyber infrastructure).

were the DDoS attacks a "resort to armed force" sufficient to trigger an international armed conflict? Alternatively, should the DDoS be viewed merely as another form of a conventional attack—like any other type of military preparation of the battlefield? Should the focus be on the usefulness or effectiveness of the preparation, rather than the format (cyber)? These questions do not lend themselves to easy answers. In sum, the above gaps, ambiguities, and fault lines highlight that even the most uncomplicated scenario is strewn with uncertainty and complexity because it included cyber means and methods and occurred, at least in part, in cyberspace.

Although not one of the case studies, an interesting corollary to the Russian-Georgian international armed conflict from a cyber operations perspective was Russia's use of cyber operations against Ukraine.[112] Since July 2014, there has been an international armed conflict between Ukraine and Russia. Parenthetically, this international armed conflict is parallel to an ongoing non-international armed conflict in Ukraine.[113] And, of course, Russia occupied and then annexed the Ukrainian peninsula of Crimea in 2014.[114] From a cyber operations perspective, the most well-known incident occurred in 2015 when the electricity was cut for nearly a quarter-million Ukrainians by highly sophisticated hackers who successfully attacked a power grid. Additionally, about a year later, a transmission station was taken down through a cyberattack.[115]

---

[112] *See generally Ukraine Fast Facts*, CNN (Feb. 28, 2017), http://edition.cnn.com/2014/02/28/world/europe/ukraine-fast-facts/index.html [https://perma.cc/P34E-WAZY] (last visited Oct. 16, 2017) (providing basic factual information about Ukraine and a timeline of important developments in Ukraine's national history relating to Russia).

[113] *International Armed Conflict in Ukraine*, RULE L. ARMED CONFLICTS PROJECT (RULAC) GENEVA ACAD. INT'L HUMANITARIAN L. & HUM. RTS., (Sept. 11, 2017), http://www.rulac.org/browse/conflicts/international-armed-conflict-in-ukraine#collapse2accord [https://perma.cc/JM4G-PS3D] (last visited Oct. 16, 2017) (recognizing that the available information does suggest the existence of an armed conflict in eastern Ukraine from July 2014).

[114] *See* Daniel Treisman, *Why Putin Took Crimea*, FOREIGN AFF. (Apr. 18, 2016), https://www.foreignaffairs.com/articles/ukraine/2016-04-18/why-putin-took-crimea [https://perma.cc/7RKX-UC5H] (delineating interpretations of Putin's motives for annexing Crimea).

[115] *See Was Russian Hacking of Ukraine's Power Grid a Test Run for U.S. Attack?*, CBS NEWS (June 23, 2017), https://www.cbsnews.com/news/russian-hacking-of-ukraines-power-grid-test-run-for-us-attack/ [https://perma.cc/RS8X-WU89]

Since then, there has been a growing roster of Ukrainian companies and government agencies that have been plagued by cyberattacks, often being hit in rapid succession.[116] Additionally, cyber security experts detected a malware implant on Android devices which was used to track the movements of Ukrainian artillery units and then target them. The significance of such a cyberattack is obvious. Hackers were able to access the communications of its adversaries and the geolocations of the devices themselves, which enabled Russia to effectively target Ukrainian artillery.[117] Unsurprisingly, the Ukrainians accused the Russians of these cyber operations. Oleksandr Tkachuk, the Chief of Staff for Ukraine's Security Service, alleged that the cyberattacks were coordinated by the Russian security service with assistance from private software firms and criminal hackers. Moscow has repeatedly and persistently denied accusations that it has engaged in cyber operations against Ukraine.[118]

The Stuxnet case study also raises the question of whether the cyber operation against SCADA systems at an Iranian nuclear fuel processing plant triggered an international armed conflict under IHL.[119] The Stuxnet case is different from the previous situations of

---

(examining Russia's desire to destabilize Ukraine through its power grid as a warning to the U.S.).

116 *See, e.g.*, Andy Greenberg, *How an Entire Nation Became Russia's Test Lab for Cyberwar*, WIRED (June 20, 2017), https://www.wired.com/story/russian-hackers-attack-ukraine/ [https://perma.cc/NV5N-9WWA] (addressing Russia's use of Ukraine as a laboratory for perfecting new forms of global online combat).

117 *See* Shaun Walker, *Group Allegedly Behind DNC Hack Targeted Ukraine, Report Finds*, GUARDIAN (Dec. 22, 2016), https://www.theguardian.com/technology/2016/dec/22/dnc-hack-crowdstrike-ukraine-malware-russia [https://perma.cc/HV45-J6NW] (describing the electronic attack on Estonia conducted by a pro-Kremlin youth group).

118 *See* Natalia Zinets, *Ukraine Charges Russia with New Cyber Attacks on Infrastructure*, REUTERS (Feb. 15, 2017), https://www.reuters.com/article/us-ukraine-crisis-cyber/ukraine-charges-russia-with-new-cyber-attacks-on-infrastructure-idUSKBN15U2CN [https://perma.cc/5AK8-99YF] (elaborating on the use of Telebots, a new mechanism to infect computers that control infrastructure, and Moscow's continued insistence that it is not responsible for cyberattacks against Ukraine).

119 Beyond any *jus in bello* questions, the Stuxnet case also raises *jus ad bellum* issues. More specifically, did the Stuxnet attack meet the threshold for an armed attack under Article 51 of the United Nations Charter? Even if one disagrees that

violence involving Russia and Georgia/Ukraine in some important respects. First, the cyber operation against Iran was not linked to a conventional operation, but was exclusively cyber. To put a finer point on it, the Stuxnet virus was created and used to avoid a kinetic strike against the Iranian plant.[120] However, Stuxnet was distinguishable from some other cyber operations in that it caused physical damage. With respect to the specific question of whether the Stuxnet virus triggered an international armed conflict, there are queries about both the "international" and "armed" elements. On the international element, no State, including Russia, has ever officially acknowledged that they were responsible for the attack. Much has been written and reported attributing Stuxnet to the United States and Israel. As of this writing, neither State has publicly acknowledged a connection to Stuxnet. Therefore, it is difficult to conclusively and officially state who is responsible for the virus. That being said, given the sophistication and expense of the attack, it seems likely that a State was involved. As to the "armed" element, the Experts contributing to *Tallinn Manual 2.0* were divided as to whether the damage to the centrifuges was sufficient to meet the armed requirement, and therefore could not make a ruling regarding whether the actor was "armed." Consequently, it is very difficult to conclusively determine that Stuxnet amounted to an international armed conflict under IHL.

The third case study that has a possible nexus to common Article 2 and an international armed conflict is the 2007 Estonia DDoS incident. The Estonians initially believed that the Russians launched the cyberattacks against them for several reasons. First, the cyberattacks appeared to be linked to the relocation of a Soviet Red Army soldier memorial thereby pointing to a motive.[121] Second, all

---

the Stuxnet virus amounted to an armed attack, it clearly met the threshold for prohibited use of force under Article 2(4) of the U.N. Charter.

[120] KAPLAN, *supra* note 49, at 204. *See also* The Editors, *Here's How to End the Fog of Cyber War*, SCI. AM. (June 1, 2016), https://www.scientificamerican.com/article/here-s-how-to-end-the-fog-of-cyber-war/ [https://perma.cc/7ACE-32AC] (describing the agendas international entities and countries are pushing to create a cybertruce and cooperate during cybercrime investigations).

[121] *See* McGuinness, *supra* note 38 (identifying Russia as potentially responsible for the cyberattack while acknowledging that the identification is unproven and makes retaliation difficult).

of the websites that were targeted by the DDoS attacks were in Estonia. Third, Russian websites were used in planning, facilitating and coordinating the cyberattacks. Fourth, those who planned and coordinated the attacks were fluent in Russian. Fifth, Estonian authorities traced Internet addresses used in the attacks back to Russian government agencies.[122] Finally, Estonian appeals to Moscow for assistance were ignored.[123] The culprits of the attacks were ultimately believed to be a small group of Russian patriotic hacktivists associated with the pro-Kremlin youth group called Nashi ("Ours"), engaged in an online political protest.[124] However, based off these facts, under IHL, the 2007 Estonian DDoS attack did not rise to the level of an international armed conflict for two reasons.

First, there is insufficient evidence that Nashi or other hacktivists who perpetrated the attack were operating pursuant to instructions of the Russian government or under Russian direction or control. As a practical matter, it is very difficult to prove that a State is controlling a non-State group with respect to the group's actions in cyberspace.[125] This is especially true when, like the present case, Russia never endorsed or adopted the conduct.

Second, it would be difficult to say that a DDoS attack by itself meets the threshold of "armed" under common Article 2. As noted by the Experts to the *Tallinn Manual 2.0*, the conduct of hostilities under IHL presupposes a collective application of means and methods of warfare.[126] Of course, this begs the harder question --

---

122 SUSAN W. BRENNER, CYBERTHREATS: THE EMERGING FAULT LINES OF THE NATION STATE 85–86 (2009).

123 *See* McGuinness, *supra* note 38 (explaining how Estonia created the voluntary, "shadowy" Cyber Defence unit in response to Russia's unwillingness to provide assistance).

124 *See* Andrew Roche, *Kremlin Loyalist Says Launched Estonia Cyber-Attack*, REUTERS (Mar. 13, 2009), https://www.reuters.com/article/us-russia-estonia-cyberspace/kremlin-loyalist-says-launched-estonia-cyber-attack-idUSTRE52B4D820090313 [https://perma.cc/9HU7-TEXS] (providing more details on the pro-Kremlin group, Nashi, which is responsible for the electronic attack on Estonia that paralyzed the state's Internet network).

125 TALLINN MANUAL 2.0, *supra* note 20, at 380 (noting that if a State merely supports the actions of a non-State group, that is insufficient to internationalize the situation. Under IHL, the threshold for internationalizing a conflict remains a high one).

126 *Id.* at 383.

does there have to be a threshold of requisite violence to meet the "armed" criteria to trigger IHL under common Article 2? As mentioned previously, the commentary to the Third Geneva Convention makes clear there is no intensity requirement. The drafters of the 1949 Geneva Conventions intended the threshold of international armed conflict to be low to ensure IHL applied when States were resorting to armed force against each other.[127] By having a low threshold, the conflict would be subject to the international rule of law and the victims of the conflict would benefit from humanitarian protections. Of course, the 1949 Geneva Conventions were drafted and the 1960 commentary was written well before anyone could envision cyber operations and DDoS attacks. Those who believe there should be an intensity requirement point to State practice. This practice indicates there have been a number of incidents, such as sporadic border incidents or naval incidents that were not treated or characterized as international armed conflicts.[128] Professor Gary Solis characterizes such incidents as armed conflicts short of war and contends persuasively that such incidents do not trigger an international armed conflict. Professor Solis also noted that a "key *indicium* [is] whether the incident is protracted. The longer an incident continues, the more difficult it is to describe it as merely an incident."[129] By analogy, a single DDoS attack that causes only limited damage, destruction, injury, or death would not necessarily be considered a trigger for an international armed conflict.

Candidly, there are some good arguments that the DDoS attacks in Estonia might have risen to the level of an "armed conflict." Chief among these arguments is the intensity of the attacks and their protracted nature. The incident lasted weeks and targeted both public and private sectors. For one of the most wired countries in the world like Estonia, a sustained, two-week DDoS incident is more than just an inconvenience. Arguably, if Estonia had not been as sophisticated and adept at defending itself as it proved to be, the 2007 DDoS attacks would have been far more devastating.[130] However, the greater weight of the available evidence militates

---

127 Commentary, GC III, *supra* note 105, at 22–23.

128 TALLINN MANUAL 2.0, *supra* note 20, at 383.

129 SOLIS, *supra* note 23, at 162.

130 BRENNER, *supra* note 122, at 85.

against such a conclusion. Ultimately, the hostilities that took place in Estonia did not constitute the "collective application of means and methods of warfare" sufficient to constitute an "armed conflict." Thus, the Estonia incident cannot fairly be characterized as an international armed conflict and, therefore, IHL does not apply.[131] The primary reason for this conclusion is that the connection between Nashi and the Russian government was too nebulous and the purposefully high threshold for internationalizing an armed conflict was not met.

In sum, whether a particular situation amounts to an international armed conflict under common Article 2 depends upon a totality of the circumstances. Such determinations are often quite subjective and challenging, particularly when considering incidents involving new means, methods, and domains of warfare like cyber. The next step in the multi-tier analysis is to consider non-international armed conflicts.

5. COMMON ARTICLE 3: NON-INTERNATIONAL ARMED CONFLICTS

Non-international or internal armed conflicts are armed conflicts that do not occur between States. From a humanitarian perspective, the victims of international and non-international armed conflicts face similar problems and need similar protections.[132] In some cases, the savageness and brutality of civil wars are even greater than those of international armed conflicts.[133] For combatants or fighters conducting hostilities in the context of international or non-international armed conflicts respectively, the distinction between the two types of conflicts may seem academic and quite divorced from reality. States, on the other hand, have never agreed to treat international and non-international armed conflicts equally.[134] Generally speaking, since the 1648 Peace of Westphalia, acts of sovereign leaders within their own territory have not been matters

131 TALLINN MANUAL 2.0, *supra* note 20, at 382.

132 SASSÒLI, BOUVIER & QUINTIN, *supra* note 27, at 323.

133 KOLB & HYDE, *supra* note 20, at 66.

134 SASSÒLI, BOUVIER & QUINTIN, *supra* note 27, at 323.

for international concern or regulation.[135] States have always considered non-international armed conflicts internal affairs regulated by domestic laws.[136] As mentioned above, prior to the adoption of the 1949 Geneva Conventions, International Humanitarian Law (IHL) was only intended to regulate wars between States with the limited exception of belligerency. The initiation and waging of war was an exercise of sovereign power held by States.[137] Treating an internal conflict as 'war' and subjecting it to international norms would have unduly elevated the status of those perpetrating violence as non-state actors.

The sea change occurred with the addition of common Article 3 to the 1949 Geneva Conventions. Common Article 3, sometimes referred to as the "convention in miniature," may be the most significant innovation to the 1949 Geneva Conventions because it established baseline humanitarian protections for the victims of non-international armed conflicts.[138] Prior to 1949, there were no codified provisions of IHL that specifically addressed non-international armed conflicts.[139] Common Article 3 was the first of its kind. Specifically, it provides as follows:

> 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:
>
> (1) 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, without any adverse distinction founded on race, colour, religion or faith, sex, birth or wealth, or any other similar criteria.

---

135 SOLIS, *supra* note 23, at 104.

136 SASSÒLI, BOUVIER & QUINTIN, *supra* note 27, at 324.

137 2016 COMMENTARY, GC I art. 3, *supra* note 74.

138 SOLIS, *supra* note 23, at 104.

139 ANTHONY CULLEN, THE CONCEPT OF NON-INTERNATIONAL ARMED CONFLICT IN INTERNATIONAL HUMANITARIAN LAW 25 (2010) (noting the absence of substantive international humanitarian law relating to non-international armed conflicts).

> To this end, the following acts are and shall remain prohibited at any time and in any place whatsoever with respect to the above-mentioned persons:
>
> (a) violence to life and person, in particular murder of all kinds, mutilation, cruel treatment and torture;
>
> (b) taking of hostages;
>
> (c) outrages upon personal dignity, in particular humiliating and degrading treatment;
>
> (d) the passing of sentences and the carrying out of executions without previous judgment pronounced by a regularly constituted court, affording all the judicial guarantees which are recognized as indispensable by civilized peoples.
>
> (2) The wounded and sick shall be collected and cared for.
>
> An impartial humanitarian body, such as the International Committee of the Red Cross, may offer its services to the Parties to the conflict. The Parties to the conflict should further endeavour to bring into force, by means of special agreements, all or part of the other provisions of the present Convention.
>
> The application of the preceding provisions shall not affect the legal status of the Parties to the conflict.[140]

The protections of common Article 3 were supplemented in 1977 with Additional Protocol II to the 1949 Geneva Conventions.[141] Classifying non-international armed conflicts is more difficult than international ones. There are several reasons for this conclusion.

---

[140] Geneva I, *supra* note 79, art. 3.

[141] International Committee of the Red Cross ("ICRC"), Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II), 8 June 1977, 1125 UNTS 609, http://www.refworld.org/docid/3ae6b37f40.html [https://perma.cc/2WYD-HPVU]. Additional Protocol II ("AP II") has only 28 articles and is not substantively controversial. Its material field of application is set to a high threshold. To trigger the application of Additional Protocol II, the dissident armed forces or other organized groups must exercise such control over a part of the territory of the State as to enable them to carry out sustained and concerted military operations. The U.S. has not ratified AP II, but many of its principles are recognized as customary international law. Common Article 3 does not have a similar "territorial control" requirement.

First, States are generally reluctant to classify situations of violence in their territory as non-international armed conflicts for fear that doing so would not only legitimize a group or groups fighting against the government, but also because it would trigger international regulation under IHL. The second reason why it is more difficult to classify non-international armed conflicts stems from the definition of the term itself. Common Article 3 defines a non-international armed conflict in the negative. A non-international armed conflict is defined as a conflict that is "not of an international character". It is defined in contradistinction to an international one, as opposed to being a conflict in its own right. A third point is that there are situations of violence that occur within a State that fall below the threshold of an armed conflict. These include: riots, criminality, and sporadic acts of violence that do not trigger a non-international armed conflict. Again, because "armed conflict" was never defined in the corpus of IHL, the threshold for a non-international armed conflict developed through international case law. Not surprisingly, in its landmark *Tadić* case, ICTY set forth two criteria for a non-international armed conflict. These criteria reflect customary international law: intensity of the hostilities and organization of the armed group.[142] The ICTY stated, in the pertinent part, as follows:

> The test applied by the Appeals Chamber to the existence of an armed conflict for the purposes of the rules contained in Common Article 3 focuses on two aspects of a conflict; the intensity of the conflict and the organization of the parties to the conflict. In an armed conflict of an internal . . . character, these closely related criteria are used solely for the purpose, as a minimum, of distinguishing an armed conflict from banditry, unorganized and short-lived insurrections, or terrorist activities, which are not subject to international humanitarian law.[143]

Similar to international armed conflicts, there are a number of issues raised when looking at non-international armed conflicts

---

[142] *See* TALLINN MANUAL 2.0, *supra* note 20, at 387 (explaining that the holding of is "widely accepted as seeting forth the two key criteria for qualification as a non-international armed conflict").

[143] SOLIS, *supra* note 23, at 164 (citation omitted).

through the lens of cyber operations. The starting point for such an analysis is Rule 83 of *Tallinn Manual 2.0*, which acknowledges that non-international armed conflicts may include or be limited to cyber operations between governmental armed forces and organized groups or between one or more organized groups (without the involvement of governmental armed forces).[144] Rule 83, which is also a reflection of customary international law, reiterates that the protracted armed violence must meet the *Tadić* criteria.[145] As a threshold matter, the Experts in *Tallinn Manual 2.0* recognized that, in theory, cyber operations alone, without kinetic actions, could trigger a non-international armed conflict because the application of IHL does not depend upon a specific type of military operation, or a particular means or method of warfare.

They did note, however, that this would be an "exceptional" case because of the threshold of violence required and the level of organization of the group resorting to such violence.[146] In terms of the organization requirement, which is a factual, context specific determination, the ICTY commented that the non-State armed group does not have to have the organizational structure of a State party's conventional military unit. Some degree of organization by the non-State armed group will be sufficient to meet the standard.[147] There are a number of factors that may be helpful in making such a determination: the organization and structure of the armed group, the use of internal regulations; the capacity to engage in coordinated military operations; the ability to provide military training, and the ability to enforce discipline and ensure compliance with IHL.[148] The significance of these criterion is that it would preclude lone hackers,

---

144 *See* TALLINN MANUAL 2.0, *supra* note 20, at 385 (setting forth Rule 83: "A non-international armed conflict exists whenever there is protracted armed violence, which may include or be limited to cyber operations, occurring between governmental armed forces and organized armed groups, or between such groups").

145 *Id.*

146 *Id.* at 385–86.

147 NICHOLAS TSAGOURIAS & RUSSELL BUCHAN, RESEARCH HANDBOOK ON INTERNATIONAL LAW AND CYBERSPACE 337 (2015) (arguing that the transcendental nature of cyber warfare reignites the disagreement as to whether common article 3 places a spatial element on non-international armed conflict, therefore limiting its' the geographical scope).

148 *Id.* at 338.

or even individuals ideologically sympathetic to a particular cause acting collectively but not as a coordinated entity, from meeting the organizational requirement.[149]

The larger question is whether "virtual groups" that organize exclusively online could meet the organization criteria. Even though such groups are able to carry out cyber operations in a coordinated matter, most commentators believe that such groups are not sufficiently organized to meet the *Tadić* organization requirement. The reason is simple -- virtual groups lack the ability to enforce discipline and ensure compliance with IHL.[150] They have no physical control over their members. The classic example of such a group is the collective "Anonymous." This decentralized group of international hacktivists has been linked to a number of high-profile incidents, including internet attacks on governments, major corporations, financial institutions and religious groups.[151] Notwithstanding their effectiveness and high profile, Anonymous would arguably not meet the criteria for a non-State armed group under IHL because it does not possess the ability to enforce discipline within its membership, nor to ensure that its members comply with IHL. Of course, virtual groups raise thought-provoking questions like the extent to which the capacity to enforce rules and discipline is a critical component of an organization for classification purposes. Another good question is whether physical control is a necessary precondition for the purpose of organization.

The second requirement for determining whether an episode of violence constitutes the initiation of a non-international armed conflict is the intensity of the violence. As previously mentioned, for the purpose of triggering a non-international armed conflict, the hostilities between the parties must reach a certain level of intensity.[152] Criteria indicating a sufficient intensity level would include, but are not limited to: the gravity and frequency of attacks,

---

149 *Id.*

150 *Id.*

151 Geneva Sands, *What to Know About the Worldwide Hacker Group 'Anonymous,'* ABC NEWS (Mar. 19, 2016), http://abcnews.go.com/US/worldwide-hacker-group-anonymous/story?id=37761302 [https://perma.cc/D3M7-PY5T] (detailing the identity and principles of the hacker group "anonymous", specifically focusing on the manner in which broad membership runs the gamut of the organization).

152 TSAGOURIAS & BUCHAN, *supra* note 147, at 340.

the temporal and territorial expansion of the violence; the collective nature and scope of the hostilities; the control of the territory by the non-State armed group, the number and type of governmental forces responding to the violence; the type and distribution of weapons used by the armed group; the extent to which the population has been effected or displaced by the hostilities; and whether the situation of violence has come to the attention of the United Nations Security Council.[153] In the Commentary to Rule 83, the Experts provided a non-exhaustive list of activities that would not meet the intensity requirement, including but not limited to: network intrusion, the deletion or destruction of data, computer network exploitation, defacing websites, data theft, as well as the blocking of certain Internet functions or services.[154]

With respect to intensity, one of the issues the Experts struggled with was whether a non-destructive, but severe, cyber operation could cause a violent situation to transform into a non-international armed conflict.[155] Necessarily intertwined with this is the question of whether this same situation would trigger the application of common Article 3.[156] Such a cyber operation coupled with other actions could cumulatively surpass the intensity threshold for a non-international armed conflict. For example, suppose a non-State armed group conducts a cyber-attack against a State's armed forces and exploits and destroys data vital to the defense of the State. That cyber operation, coupled with certain physical acts of violence, could certainly tip the balance and transform a situation of violence into a non-international armed conflict.[157]

---

153 *Id.* at 340–1.

154 TALLINN MANUAL 2.0, *supra* note 20, at 388.

155 *Id.* at 389. Depending on the specific factual circumstances, it may also trigger Additional Protocol II.

156 *Id.*

157 Conversation with Tomas Minarik, Senior Research at the NATO CCD COE (October 15, 2017). Left unanswered, however, is whether a cyberattack that is not coupled with certain physical acts of violence could transform a situation of violence into a non-international armed conflict. For example, if a non-State entity used cyber means to map out the strength, capabilities, and disposition of its adversary's armed force for potential use in a future attack, would the extensiveness of the intrusion and the sensitivity of the information collected suffice to meet the intensity threshold? Or would it depend upon the occurrence of a subsequent attack?

The last case study involving ISIS illustrates a non-international armed conflict which involved the use of cyber operations. To provide greater context, the armed conflict involving ISIS in Syria, Iraq, and elsewhere in the world is complex and difficult to classify, in part, because of all of the contending parties involved, State and non-State. Although sorting out the nuances of all of the conflict classification issues with ISIS is well beyond the scope of this article, it is fair to say that most of the hostilities involving ISIS are non-international armed conflicts because ISIS is a non-State armed group.[158] With ISIS, there is no doubt that they meet the *Tadić* intensity and organizational criteria.[159] To the degree that there is an issue, it relates to the geographical scope of the non-international armed conflict. In 2016, the United States National Counterterrorism Center reported that the Islamic State was operational in 18 different countries around the world. It also found indications of what it characterized as "aspiring branches" in Mali, Egypt, Somalia, Bangladesh, Indonesia, and the Philippines.[160] As will be discussed below in more detail, the geographical dimensions of non-international armed conflicts are difficult to conceptualize in the context of cyber operations.[161] Beyond the specific issues associated with cyber operations in common Articles 2 and 3, there are also gaps, ambiguities, and fault lines inherent in conflict classification under IHL, *writ large*.

---

158 *See* David Wallace, Amy McCarthy, & Shane 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. (Aug. 21, 2017) (detailing the actors involved in the Syrian Civil War and classifying them under international law, including ISIS).

159 *See* Christopher Woody, *US Special Operations Command Chief Claims '60,000 to 70,000' ISIS Fighters Have Been Killed*, BUSINESS INSIDER (Jul. 24, 2017), http://www.businessinsider.com/gen-raymond-thomas-socom-60000-to-70000-isis-fighters-killed-2017-7 [https://perma.cc/35QA-FBUV] (detailing that at any given time, it is difficult to determine how many fighters belong to ISIS. "In 2014, an observer group estimated the terror group had 100,000 fighters. The Pentagon said in summer 2016 that it had just 15,000 to 20,000 fighters left in Iraq and Syria.") *Id*.

160 *See* ISLAMIC STATE AND THE CRISIS IN IRAQ AND SYRIA IN MAPS, BBC NEWS, http://www.bbc.com/news/world-middle-east-27838034 [https://perma.cc/PX6D-5HYY] (last visited Oct 8, 2017) (explaining the results of recapturing Iraq and Syria territory which were previously claimed by jihadist groups).

161 *See* TALLINN MANUAL 2.0, *supra* note 20 at 378 (describing geographical limitations on the law of armed conflict).

6. CONFLICT CLASSIFICATION AND CYBER: GAPS, AMBIGUITIES, AND FAULT LINES

The binary classification paradigm established by the 1949 Geneva Conventions goes to the very heart of the regulation of armed conflicts. As presented above, cyber operations pose several challenging issues with respect to the application and interpretation of common Articles 2 and 3. Beyond those specific issues, there are a number of overarching complexities that create gaps, ambiguities, and fault lines with respect to applying IHL to cyber operations generally and to issues related to conflict classification specifically. The first involves the problem of attribution.

Attribution is considered an intractable theoretical and practical problem permeating every aspect of cyber operations. Commenting on attribution, author Joel Brenner wistfully observed that, "the internet is one big masquerade ball. You can hide behind aliases, you can hide behind proxy servers, and you can surreptitiously enslave other computers to do your dirty work."[162] Hence, attribution creates technical, policy and legal issues. From a technical perspective, attribution can be utterly perplexing because hackers have tools, tactics, and techniques that effectively and efficiently cover their tracks. One method a cyber intruder can use is a so-called botnet. Botnets are a network comprised of computers remotely controlled by an intruder to conduct coordinated cyber operations. With no practical limit to the number of bots that can be assimilated into a botnet, it could become extremely difficult to know the origin of any given cyber operation.[163]

From a policy perspective, some influential thought leaders have argued that there is a misplaced "attribution fixation" for many who believe that attribution must start at the lowest, most technical levels. They argue persuasively that it is necessary to take one step back and think more broadly about attribution. Under this argument, the focus should be placed on those things that decision-

---

[162] *See* Marco Roscini, *Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations* in CYBER WAR: LAW AND ETHICS FOR VIRTUAL CONFLICTS 215 (Jens David Ohlin et al. eds., 2015) (explaining that evidentiary problems in inter-state litigation are not peculiar to cyber operations).

[163] *See* TALLINN MANUAL 2.0, *supra* note 20 at 563 (describing neutrality and Security Council actions).

makers actually need to know about a cyber-attack. What they really need to know is who is ultimately responsible for the attack. Knowing who actually pressed the keys is not necessarily dispositive or particularly helpful unless it leads to insights into who is ultimately culpable for the attack.[164] Finally, with respect to attribution and the law, there are many challenging issues. The Experts who worked on *Tallinn Manual 2.0* agreed, as a general matter, regarding the *ex ante* uncertainty as to the attribution of cyber operations, noting:

> States must act as reasonable States would in the same or similar circumstances when considering responses to them [cyber attacks]. Reasonableness is always context dependent. It depends on such factors as reliability, quantum, directness, nature (*e.g.*, technical data, human intelligence), and specificity of the relevant available information when considered in light of the attendant circumstance and the importance of the right involved. These factors must be considered together. Importantly in the cyber context, deficiencies in technical intelligence may be compensated by, for example, the existence of highly reliable human intelligence.[165]

In terms of the classification of international and non-international armed conflicts, the problem is somewhat obvious. Under IHL, conflict classification is premised on the assumption that the identity of one's adversary is known.[166] To the degree, conflict classification issues arose regarding attribution, it typically involved the question of whether the conduct of a non-State armed group was legally attributable to a State. As discussed above, that is an important issue because it could have the effect of internationalizing the armed conflict thereby placing it under common Article 2 instead of common Article 3. The outcome of this analysis could also

---

[164] *See* Jason Healy, *The Spectrum of National Responsibility for Cyberattacks*, 18 BROWN J. OF WORLD AFF. 43–56, 43 (2011) (explaining that the cyberdefense community must accept the idea that national policy makers need to know the responsibility for an attack).

[165] *See* TALLINN MANUAL 2.0, *supra* note 20, at 82 (describing the law of international responsibility for wrongful acts by a State).

[166] *See* TSAGOURIAS & BUCHAN, *supra* note 147, at 332 (explaining how to classify cyber warfare).

mean the conduct at issue is not covered by IHL at all. Of course, the attribution issue goes beyond the non-State actors being *de facto* agents for States. The ability of State and non-State armed groups to be virtually anonymous in carrying out cyber operations is a reality; put more prosaically --"electrons don't wear uniforms."[167] States targeted with cyber operations often find their response options severely limited in the absence of an identifiable perpetrator of the operations.[168] Logically, absent the ability to attribute the cyber operation to a State party or non-State armed group, conflict classification is impossible.[169] Future advancements in technology may make attribution easier. But, as it stands now, attribution efforts are often enormously time-consuming and require extensive technical and non-technical investigative means and analytical techniques to gather, preserve, and analyze the evidence.[170]

The second issue concerns the current status of the binary classification paradigm and how that relates to cyber operations. In many ways, the binary conflict classification paradigm and the consequences that flow from it has evolved both substantively and procedurally over the last seven decades. First, in terms of substance, there has been a general tendency to reduce the differences between the rules that are applicable to international and non-international armed conflicts.[171] This trend toward convergence to more of a unitary legal standard under IHL can be seen in the jurisprudence of international criminal tribunals, the influence of human rights laws and even some international agreements that specify the application in international and non-

---

[167] *See* NAT'L RES. COUNCIL OF THE NAT'L ACADS., *supra* note 19, at 139 (describing how to characterize an incoming cyberattack and its attribution).

[168] *See* Michael N. Schmitt & Liis Vihul, *Proxy Wars in Cyber Space: The Evolving International Law of Attribution*, FLETCHER SECURITY REVIEW 55 (2014) (describing that a multilevel legal analysis is required in order to attribute cyber activities of a non-state group or individual, or even in some cases another state to a state as a matter of international law).

[169] This assumes, of course, there is no conventional or kinetic "resort to armed force" that could be used as the basis to classify a conflict.

[170] *See* TSAGOURIAS & BUCHAN, *supra* note 147, at 332 (explaining how to classify cyber warfare).

[171] *See* SASSÒLI, BOUVIER & QUINTIN, *supra* note 27, at 124 (describing general protection of populations against certain consequences of war).

international armed conflicts.[172] Commenting on this movement toward convergence, an ICRC publication stated, in part, as follows:

> [I]t has even been suggested in some quarters that the differences be eliminated altogether. In the many fields where the treaty rules still differ, this convergence has been rationalized by claiming that under customary international law the difference between the two categories of conflict has gradually disappeared. The ICRC study on Customary International Humanitarian Law comes, after ten years of research, to the conclusion that 136 (and arguably even 141) out of 161 rules of customary international humanitarian law, many of which are based on rules of Protocol I applicable as a treaty to international armed conflicts, apply equally to non-international armed conflicts.[173]

Although far from settled or agreed upon, there is certainly some logical appeal to the notion that there is a substantive body of customary IHL that applies to both international and non-international armed conflicts.[174] Encapsulating this notion, in *Tadić*, ICTY noted that, "what is inhumane and consequently proscribed, in international wars, cannot but be inhumane in civil strife."[175] However, it is highly unlikely there will ever be a complete convergence of the IHL governing international and non-international armed conflicts. The reason is simply that States will never agree to combatant status for members of non-State armed groups fighting against governments in non-international armed conflicts. To provide such a status would mean that such fighters would have combatant immunity and be entitled to prisoner of war status upon capture. It is simply unfathomable States would go that far even if driven by altruistic humanitarian impulses or more pragmatic concerns like encouraging reciprocity by the insurgents. From a conflict classification perspective, the significance of convergence is that it leaves an erroneous impression that the

---

172 *Id.*

173 *Id.*

174 *See* EMILY CRAWFORD & ALISON PERT, INTERNATIONAL HUMANITARIAN LAW 71 (2015) (explaining that conditions set out in Article 1 mean that the Protocol's scope of application is narrower than that of Common Article 3).

175 *Id. citing Tadić* Jurisdiction, paras. 117–26.

distinction between international and non-international armed conflicts is not vitally important. This false impression may be exacerbated when the conflict at issue is limited to or primarily conducted by cyber operations, which already lack the traditional feel of a conventional armed conflict.

Notwithstanding the concerns mentioned above, the most significant issues are procedural[176] in nature. That is, hostilities over the past two decades are not always easily or neatly classified as either an international or non-international armed conflict as was envisioned and proscribed by the 1949 Geneva Conventions. For example, some scholars have progressively theorized that, in addition to international and non-international armed conflicts, there are now "transnational armed conflicts" which have been born out of State practice. This type of conflict arguably emerged from counter-terror military operations between States and non-State groups outside the territory of the State.[177] There are also mixed conflicts that have both internal and international characteristics. Such conflicts may require a legal determination as to conflict classification at each particular phase of the operation to ensure the correct portion of IHL is being applied.[178] Additionally, there are some situations that have been characterized as "armed conflicts short of war."[179] This category might encompass a border or coastal incident between States involving limited, short-lived violence. There are also situations of violence in an ungoverned territory in failed States that may create conflict classification challenges. And,

---

176 In this context, the term "procedural" is intended to frame how and when the substantive rules apply. For example, procedurally, common Article 2 and common Article 3 delineate which rules apply under given circumstances. Substantively, this means that individuals taking part in a conflict deemed to be an international armed conflict (and, therefore, governed by common Article 2) would be accorded the status of "combatant."

177 *See* Geoffrey S. Corn & Eric Talbot Jensen, *Transnational Armed Conflict: A 'Principled' Approach to the Regulation of Counter-Terror Combat Operations,* 42 ISRAEL L. REV. 46 (2009) (explaining that LOAC principles must be identified and must be broad enough to provide the authority necessary to bring the transnational enemy to submission).

178 *See* Akande, *supra* note 62, at 63 (providing the example of intervention by multinational forces under UN command or authorized by the UN).

179 *See* SOLIS, *supra* note 23, at 161 (including cross-border terrorist attacks by non-state Actors).

of course, there is cyber warfare. Commenting on the procedural challenges associated with cyber operations, Professor Schmitt observed:

> In the future, cyber warfare will further complicate classification. Cyber operations have the potential for producing vast societal and economic disruption without causing physical damage typically associated with armed conflict. They are also inherently transborder, thereby frustrating any approach to classification based on geographical factors. Moreover, massive attacks can be launched by a single individual or by a group that is organized entirely online. This is in sharp contrast to traditional warfare, which depends on either the involvement of a State's armed forces or that of a group capable of mounting typical military operations.[180]

Given the above, it is clear that the traditional binary classification paradigm is being stressed both substantively and procedurally. The emergence of cyber operations will only exacerbate these stresses.

A third issue relates to how traditionally-understood geographical limitations, which are part of the fabric of IHL, are to be conceptualized and considered in cyber operations. These limits are particularly germane in non-international armed conflicts. That is, the geographical scope of non-international armed conflicts under common Article 3 has been a matter of intense debate for some time. One view is that the plain language of common Article 3 signifies that non-international armed conflicts are limited to the territory of a single State. This is the most restrictive approach.[181] It traces its origin to the first sentence of common Article 3 which seems to limit the application of the rule to armed conflicts "not of an international character occurring in the territory of one of the

---

[180] *See* Schmitt, *supra* note 28, at 246 (explaining that cyber operations have the potential for producing vast societal and economic disruption without causing the physical damage).

[181] *See* Michael N. Schmitt, *Charting the Legal Geography of Non-International Armed Conflict*, 90 INT'L L. STUDIES 1, 9 (2014) (explaining that according to the most restrictive approach to the geographical scope of non-international armed conflict based on Common Article 3, conflicts take place within a State's geopolitical borders).

High Contracting Parties."[182] Going beyond the specific language of common Article 3, non-international armed conflicts have traditionally been understood to be conflicts occurring within the confines of a particular State. Such conflicts are also referred to as "internal" armed conflicts.[183] A logical inference under this interpretation is that an armed conflict that crosses State borders becomes an international armed conflict.[184]

A second, more palatable position is that the word "one" in the first sentence of common Article 3 refers to any of the State parties to the 1949 Geneva Conventions.[185] Given that the 1949 Geneva Conventions are the most ratified treaty in the history of the world (with every recognized State in the world having ratified all four conventions),[186] the phrase would impose no territorial limitation.[187] Additionally, as noted in the 2016 Commentary to common Article 3, the object and purpose of the article supports its application beyond the territory of one State. That is, the aim of common Article 3 is to provide persons not participating or no longer actively participating in hostilities with baseline humanitarian protections during non-international armed conflicts. Therefore, it is logical that those same protections would apply when such situations of violence span the territory of more than one State.[188] As such, it is possible to have a non-international armed conflict against ISIS that spans many countries. Of course, when one considers the above debate in light of cyber operations, the fault lines are somewhat obvious. More specifically, cyber operations in furtherance of and closely related to non-international armed conflicts can be launched

---

182 Geneva I, *supra* note 79, art. 3.

183 *See* Commentary, GC III, *supra* note 105, at 455 (commenting that non-international armed conflicts have been understood as conflicts occurring within the limits of a single states, which are described as "internal" armed conflicts).

184 TALLINN MANUAL 2.0, *supra* note 20, at 386. This presumes that both parties are States, or a State and a proxy of another State.

185 *Id.*

186 SOLIS, *supra* note 23 at 88.

187 *See* TALLINN MANUAL 2.0, *supra* note 20, at 386 (explaining that the phrase imposes no territorial limitations so long as the relevant States are Parties to the Conventions).

188 *See* 2016 COMMENTARY, GC I, *supra* note 74, at 467 (discussing the purpose of common Article 3 which leads to providing persons with protections when violence spans beyond the territory of one State).

remotely, far removed from the territory in which the conventional hostilities are happening.[189] The *Tallinn Manual 2.0* Experts "acknowledged the existence of a narrower approach that accepts the possibility of a non-international armed conflict that crosses borders, but which imposes a requirement of geographical proximity to the State involved in the conflict."[190]

Additionally, in interpreting common Article 3, questions have been raised as to whether IHL applies to the entire territory of a State in which a non-international armed conflict is occurring or whether the application of the law is limited to only that portion of the State where hostilities are occurring. Put in a slightly different manner, in the regions of a State that are peaceful, do the State's criminal laws and procedures provide a sufficient legal framework?[191] The *Tallinn Manual 2.0* Experts opined that in a non-international armed conflict, the application of IHL is not limited only to areas of active hostilities. Rather, IHL would apply to the entirety of the State.[192] There is,

---

[189] *See* TALLINN MANUAL 2.0, *supra* note 20, at 386–7. As noted by the Experts, some States have weak or ineffective regulatory mechanisms to prevent or stop cyber activity from occurring on their territories. Such States could be an appealing base of cyber operations for non-State actors to attack governments in other States where non-international armed conflicts are occurring.

[190] *Id*. at 382. This attempt at creating a geographical limitation does not appear workable in the cyber realm given the difficulty of attribution.

[191] *See* 2016 COMMENTARY, CG I, *supra* note 74, at 456–64 (discussing whether the application of humanitarian law concerns the whole of the State or is limited to areas where hostilities are occurring).

[192] *See* TALLINN MANUAL 2.0, *supra* note 20, at 386. There is ample support for the position of the Experts. First, the language of common Article 3 itself supports their position. It provides that "[t]o this end, the following acts are and shall remain prohibited at any time and *in any place whatsoever*." Second, in *Tadić*, the ICTY stated, in part, as follows:

> 67. . . . the temporal and geographical scope of both internal and international armed conflicts extends beyond the exact time and place of hostilities. . . .
>
> 69. . . . beneficiaries of common Article 3 of the Geneva Conventions are those taking no active part (or no longer taking active part) in the hostilities. This indicates that the rules contained in Article 3 also apply outside the narrow geographical context of the actual theatre of combat operations. . . .
>
> 70. . . . international humanitarian law continues to apply in the whole territory of the warring States or, in the case of internal conflicts, the whole

however, a practical limitation on the application of IHL anywhere in the State. That limitation is rooted in the foundational requirement that for IHL to apply there must be a nexus between the conduct in question and the armed conflict.[193]

A fourth, and final, reason for the gaps, ambiguities, and fault lines with respect to applying IHL to cyber operations concerns the "militarization" of cyberspace. There has been a great deal of discussion and debate about this issue.[194] That concern is reflected in a number of ways. For one, States are establishing military organizations that are developing cyber offensive and defensive capabilities. Cyberspace has been designated as an operational domain for warfighting purposes.[195] Important thought leaders, like Brad Smith, the President of Microsoft, called for a digital Geneva Convention in 2017. In his speech entitled, "Protecting and Defending against Cyberthreats in Uncertain Times," Smith highlighted the troubling fact that recent years have seen an expansion in the number of incidents whereby States have engaged in cyber operations against other States.[196] He forcefully argued that

---

territory under the control of a party, whether or not actual combat takes place there.

See also 2016 COMMENTARY, GC I, *supra* note 74, at 457–68 *citing* ICTY, *Tadić* Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, 1995, at 67–70 (emphasizing that once a non-international armed conflict occurs, Article 3 applies in the territory of the concerned State in its entirety).

193 *See* 2016 COMMENTARY, GC I, *supra* note 74, at 460 (noting that the applicability of humanitarian law in the whole territory of a State party to the conflict is subject to the condition that a particular act must be related to the non-intentional armed conflict).

194 *See* Sean Lawson, *Is the United States Militarizing Cyberspace?*, FORBES (Nov. 2, 2012), https://www.forbes.com/sites/seanlawson/2012/11/02/is-the-united-states-militarizing-cyberspace/#1d260267798d [https://perma.cc/QLX3-6F7R] (discussing the definition of militarizing cyberspace and whether the United States is militarizing cyberspace or not).

195 *See Cyber Defence*, NATO (Jul. 16, 2018), https://www.nato.int/cps/en/natohq/topics_78170.htm (last visited Feb. 21, 2018) [https://perma.cc/W68N-CGGL] (noting that NATO recognized cyberspace as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land and at sea).

196 *See* Brad Smith, *Protecting and Defending against Cyberthreats in Uncertain Times*, RSA Conference, https://www.rsaconference.com/videos/protecting-and-defending-against-cyberthreats-in-uncertain-times [https://perma.cc/5T8U-

the 2014 Sony attack by North Korea was a turning point.[197] In that highly publicized cyber incident, North Korean hackers stole confidential documents and data from a Hollywood studio and posted them online. U.S. government officials believe that North Korea targeted Sony because it backed the film, "The Interview," which depicts an assassination plot against the North Korean leader, Kim Jong-Un.[198] Using militaristic language and imagery, Smith described cyberspace as a new battlefield, albeit different than the other war fighting domains of land, sea, air, and space. In doing so, Smith eloquently and thoughtfully laid out arguments for a new international treaty.[199] He specifically noted:

> We need a convention that will call on the world's governments to pledge that they will not engage in cyberattacks on the private sector. That they will not target civilian infrastructure, whether it's of the electrical or the economic or the political variety. We need governments to pledge that instead they will work with the private sector to respond to vulnerabilities. That they will not stockpile vulnerabilities and they will take additional measures.[200]

The problem, of course, is that the Sony incident neither triggered the application of the 1949 Geneva Conventions, specifically, nor IHL, generally. Such violations of sovereignty fall under a peacetime international law regime. This example is illustrative of a much larger trend. That is, the vast majority of incidents that occur in cyber space between States or States and non-

---

4XAZ] (noticing the increase of nation-state cyber-attacks in recent years and discussing the ways to protect and defend against cyberthreats).

197 *Id.*

198 *See* Andrea Peterson, *The Sony Pictures Hack, Explained*, WASH. POST (Dec. 18, 2014), https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/?utm_term=.b8aac1f6ebdc [https://perma.cc/3R5V-HW4E] (detailing the events surrounding the Sony Pictures hack that lead to a leak of a large amount of confidential data and which is attributed to the North Korean government retaliating on the release of a Sony-backed film entitled "The Interview" about the assassination of the North Korean leader Kim Jong Un).

199 *Id.*

200 David Post, *Microsoft's Brad Smith on cyberattacks, cybersecurity, and 'cyberspace'*, WASH. POST (Mar. 10, 2017), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2017/03/10/microsofts-brad-smith-on-cyberattacks-cybersecurity-and-cyberspace/ [https://perma.cc/P5Q4-76CS].

State armed groups are below the threshold for an armed conflict and, therefore, do not trigger IHL. Therefore, to protect and preserve IHL for its intended purposes, cyber activities must be carefully and appropriately analysed and categorized under the IHL binary classification system. Otherwise, IHL runs the risk of being watered down and marginalized in the long run.

7. CONCLUSION

The issue of conflict classification is arguably the single most important inquiry when applying IHL. It is always the first step in establishing a framework to analyse any IHL issues. Even though the binary classification paradigm established by the 1949 Geneva Conventions is already stressed by contemporary conventional conflicts, and will be stressed even further by the emergence of cyberspace operations, the binary classification system remains the best way for the international community to conceptualize, classify, and (in some fashion, at least) control this new domain of warfare. Given the continuously-evolving nature of cyber operations, it remains all the more important to maintain a body of law that has withstood the test of time while achieving near-universal acceptance. The binary classification system within IHL remains viable. Accordingly, it should be preserved and reinforced.

There are three reasons for this conclusion. First, going back to first principles, IHL applies to cyber operations in the context of an armed conflict. With very few treaties that deal directly with cyber operations and with State practice often being highly classified,[201] it is critically important to interpret and analyze the established *lex lata* of IHL in the context of cyber operations. When it comes to IHL, there is nothing that is more foundational than common Articles 2 and 3 of the 1949 Geneva Conventions. To deviate from or marginalize the IHL conflict classification paradigm because of the novelty and nuances of cyberspace operations would be unwise. In other words, the development of IHL should be evolutionary, not revolutionary. This important work should be viewed as an effort to bring cyberspace under the mantle of existing law, not to create an entirely new framework.

---

[201] *See* TALLINN MANUAL 2.0, *supra* note 20, at 3 (noting that State cyber practice is mostly classified and that publicly available expressions of *opinio juris* are sparse).

A second, and related, point is that there is very little incentive for States to agree to anything that legitimizes non-State armed groups fighting against governmental forces. Therefore, there will always be at least two categories of armed conflict. Moreover, even though there are some unique characteristics to modern day conflicts, such as fighting against non-State groups in the territory of another State, the paradigm still procedurally works. Stressed does not mean broken. To the extent that ambiguities and gaps in the law remain, States can and should do more to clarify and facilitate the orderly and thoughtful development of IHL.

The third reason relates to the militarization of cyberspace. International humanitarian law reflects a delicate balance between military necessity and humanitarian considerations. It is a check and balance system intended to minimize human suffering without undermining military operations.[202] In some respects, the purpose of IHL – to introduce moderation and restraint in warfare – is extraordinarily difficult to achieve. Its very application is predicated upon the existence of an armed conflict. If that circumstance does not exist, it is important to recognize that other principles of international law apply to the conflict – but not IHL. This enables IHL to continue to do what it does best – regulating armed conflict – without being diluted through its application to situations that do not rise to the level of either international or non-international armed conflict.

---

[202] *See* YORAM DINSTEIN, THE CONDUCT OF HOSTILITIES UNDER THE LAW OF INTERNATIONAL ARMED CONFLICT 17 (2004) (examining the law of international armed conflict and exploring its application in hostilities such as Iraq and Afghanistan).