THE COLUMBIA
SCIENCE &
TECHNOLOGY
LAW REVIEW

VOL. XXII STLR.ORG FALL 2020

ARTICLE

SAFEGUARDING CIVILIAN INTERNET ACCESS DURING ARMED CONFLICT: PROTECTING HUMANITY'S MOST IMPORTANT RESOURCE IN WAR

Todd Emerson Hutchins*

A recent spate of governmental shutdowns of the civilian internet in a broad range of violent contexts, from uprisings in Hong Kong and Iraq to armed conflicts in Ethiopia, Kashmir, Myanmar, and Yemen, suggests civilian internet blackouts are the 'new normal.' Given the vital and expanding role of internet connectivity in modern society, and the emergence of artificial intelligence, internet shutdowns raise important questions regarding their legality under intentional law. This article considers whether the existing international humanitarian law provides adequate protection for civilian internet connectivity and infrastructure during armed conflicts. Concluding that current safeguards are insufficient, this article proposes a new legal paradigm with special protections for physical internet infrastructure and the right of civilian access, while advocating the adoption of emblems (such as the Red Cross or Blue Shield) in the digital world to protect vital humanitarian communications.

* Lieutenant Commander, JAG Corps, U.S. Navy. J.D.—U.C. Berkeley, L.L.M.–Geo. Wash. U. Special thanks to Prof. Burrus Carnahan. In honor of Prof. David Caron, who loved, inspired, and nurtured international law. The views expressed herein are the author's and do not represent the position of the U.S. Navy, Department of Defense, or U.S. government.

I. INTRODUCTION

What would happen if the internet was destroyed or inaccessible for a day, week, month, or longer? This dire hypothetical is a reality for millions of people around the world. On August 5, 2019, the Indian government shut down the internet in the contested province of Kashmir.[1] The central government stripped the area of its special autonomous status and detained prominent local leaders, sparking violent unrest.[2] Authorities claimed that military necessity warranted blocking all civilian internet access, in order to minimize "the threat of [militant Pakistan-backed rebels] misusing data connectivity" to coordinate attacks and subversive activities.[3] Foreign Minister Subrahmanyam Jaishankar asserted there were no other viable options, asking, "how do I cut off communications between the terrorists and their masters on one hand, but keep the internet open for other people?"[4]

The internet blackout sent Kashmir, a region of seven million people, into chaos, paralyzing businesses, hampering doctors seeking to consult specialists, preventing pharmacies from ordering medicine, freezing digital banking, and causing millions of online identities to be lost.[5] In the first five months of the blackout, the Kashmir Chamber of Commerce estimated that the region had lost over $1.4 billion.[6]

---

1. Niha Masih et al., *India's Internet Shutdown in Kashmir is the Longest Ever in a Democracy*, WASH. POST (Dec. 16, 2019, 2:00 AM), https://www.washingtonpost.com/world/asia_pacific/indias-internet-shutdown-in-kashmir-is-now-the-longest-ever-in-a-democracy/2019/12/15/bb0693ea-1dfc-11ea-977a-15a6710ed6da_story.html.

2. *Id.*

3. *Id.*

4. Stephen Brown & Christian Oliver, *Q and A: India's Foreign Minister on Kashmir*, POLITICO (Sept. 2, 2019, 8:50 PM), https://www.politico.eu/article/q-and-a-india-foreign-minister-subrahmanyam-jaishankar-on-pakistan-kashmir-imran-khan.

5. The popular Facebook-owned WhatsApp social messenger deleted accounts associated-data, including photos, contacts, messages, and credits automatically after 120 days of inactivity. Masih, *supra* note 1.

6. *Id.*

Tens of thousands of people became 'internet refugees,' moving or making daily trips to neighboring provinces to access the internet.[7] The shutdown lasted eight months.[8] This is not the first time Kashmir has been without internet access: authorities shut down internet access for four months in 2016 after protests erupted in response to the Indian military's killing a popular rebel leader.[9]

Elsewhere, in February 2020, Myanmar became embroiled in civil conflict against the Muslim Rohingya minority's Arakan Army and imposed a three-month-long internet blackout in Rakhine State, justifying the action as necessary due to "security requirements."[10] These recent shutdowns almost certainly will not be the last time that a government severs the civilian population's access to the internet during armed conflict.

Observers have noted that "attempts to block the internet could easily become a real part of modern warfare."[11] Yet, to date, there has been little scholarship related to protecting civilian internet access.[12] Cassondra Mix's brief study of Egypt's five-day government-imposed blackout in 2011 is one such rare work, though it focuses on a civil uprising. Mix hypothesizes that the Law of Armed Conflict (LOAC) might apply to severing civilian internet connectivity during non-international armed conflict.[13] Greater scholarly attention regarding the legality of actions which deprive civilians of internet connectivity is necessary, especially in the context of armed conflict.. As society becomes ever more digitally connected, internet access will become increasingly vital to civilian life. A new legal framework to protect civilian access to the internet in wartime is needed.

This paper aims to provide an analytic framework for policymakers, military commanders, and their legal advisors to determine whether activities that impact civilian internet access are lawful under the current international law, in addition to identifying opportunities to advance international legal protections. Part I briefly explains the vital role the internet plays in civilian life, while also explaining its vulnerability during armed conflict, by describing the means and methods that can disrupt civilian internet access. This

---

7. *Id.*

8. Software Freedom Law Ctr., India, *Longest Shutdowns*, INTERNET SHUTDOWNS, https://internetshutdowns.in (last visited Nov. 18, 2020).

9. *Id.* (referring to aftermath of Burhan Wani's killing).

10. Thu Thu Aung & Sam Aung Moon, *Myanmar Reimposes Internet Shutdown in Conflict-Torn Rakhine, Chin States: Telco Operator*, REUTERS (Feb. 5, 2020, 1:17 AM), https://www.reuters.com/article/us-myanmar-rakhine/myanmar-reimposes-internet-shutdown-in-conflict-torn-rakhine-chin-states-telco-operator-idUSKBN1ZZ0LC.

11. Cassondra Mix, *Internet Communication Blackout: Attack Under Non-International Armed Conflict*, 3 J.L. & CYBER WARFARE, Spring 2014, at 70, 73.

12. *Id.*

13. *Id.* at 72–73.

section questions whether 'flip-the-switch blackouts' and physical attacks on infrastructure should be treated differently as a matter of law, even when their resultant impact on the civilian population is the same.

Part II assesses existing protections for internet access under international law. While international human rights law (IHRL) establishes that internet access must be maintained at all times, the Law of Armed Conflict (LOAC) would, according to most scholars, apply *lex specialis*, superseding IHRL, and thereby permitting attacks on the internet as a civilian object if military commanders deem it necessary and proportionate. Furthermore, it is complex and impractical to apply traditional law of war principles—necessity, distinction, proportionality, and humanity—to military actions which impact civilian internet connectivity, due to the difficulty of weighing military advantage against the unknown impacts and repercussive effects of a widespread internet outage.

Part III begins by considering the applicability and efficacy of special protection regimes within the LOAC for humanitarian (Red Cross) and cultural (Blue Shield) purposes. It then concludes by calling for a new internet-specific protection regime within LOAC, which would include a new protective emblem (such as the red cross or blue shield in the physical world), enforcement mechanisms, submarine cable protections, and the employment of artificial intelligence and blockchain to create a 'virtual-specialized internet' for humanitarian purposes.

II. IMPORTANCE AND VULNERABILITY OF CIVILIAN INTERNET ACCESS DURING ARMED CONFLICT

A. Internet Shutdowns Pose enormous Humanitarian and Economic Costs

The importance of internet connectivity to modern humanity cannot be overstated. The world's 4.39 billion internet users spend, on average, over six hours online every day.[14] In the developed world, nearly the entire population is already online, while in the developing world over a million new users connect each day.[15] The internet has increasingly replaced print and television as a source of information.[16] Similarly, social, educational, governmental, and business interactions in much of the world are shifting online, and the coronavirus

14. Simon Kemp, *Digital Trends 2019: Every Single Stat You Need to Know About the Internet*, NEXTWEB (Jan. 30, 2019), https://thenextweb.com/contributors/2019/01/30/digital-trends-2019-every-single-stat-you-need-to-know-about-the-internet.

15. *Id.*

16. *Newspapers Fact Sheet*, PEW RES. CTR. (Jul. 9, 2019), https://www.journalism.org/fact-sheet/newspapers.

pandemic has only made this trend more apparent. Global surveys show that most people already "strongly agree that access to the internet should be considered a basic human right."[17] Philosopher Merten Reglitz claims that "Internet access is not merely a luxury . . . it is instead highly conducive to a multitude of crucial human interests and rights [for] lobbying and holding accountable global players."[18]

Disruptions to the internet cause dire impacts, especially in more connected societies with "mature online ecosystems."[19] Deloitte, a global consultancy, estimates that the cost of even a short internet shutdown in highly internet-dependent countries could be up to $23 million per day for every 10 million impacted persons.[20] In economic terms, the inability to execute day-to-day tasks reliant on internet services leads to dramatically higher transaction costs and reduced output.[21] Saipan and Tinian, for example, lost internet connectivity when an earthquake snapped the only fiberoptic cable connecting the two islands. Without internet connectivity, the islands' air traffic control was forced to ground flights, automated teller machines failed to dispense currency, and the hotel reservation systems supporting the tourist economy crashed.[22] Further, the Committee to Protect Journalism reports that internet shutdowns cut off media reports, leaving the public in the dark as to current events.[23] For example, a

17. An Internet Society survey of 10,000 people in 20 countries found that 83% felt internet access should be a basic human right. INTERNET SOC'Y, GLOBAL INTERNET USER SURVEY SUMMARY REPORT 4 (2012). Similarly, a BBC poll of more than 27,000 people in 26 countries found over 80% of internet users believe access to the internet is a fundamental right. *BBC Internet Poll: Detailed Findings*, BBC WORLD SERV. (Mar. 8, 2010), http://news.bbc.co.uk/2/hi/technology/8548190.stm.

18. Karl Bode, *The Case for Internet Access as a Human Right,* VICE: MOTHERBOARD (Nov. 13, 2019, 12:06 PM), https://www.vice.com/en_us/article/3kxmm5/the-case-for-internet-access-as-a-human-right.

19. DELOITTE CONSULTING, THE ECONOMIC IMPACT OF DISRUPTIONS TO INTERNET CONNECTIVITY: A REPORT FOR FACEBOOK 4 (2016), https://www2.deloitte.com/global/en/pages/technology-media-and-telecommunications/articles/the-economic-impact-of-disruptions-to-internet-connectivity-report-for-facebook.html.

20. *Id.* (estimating for a highly connected country).

21. *Id.* at 6.

22. Steve Weintz, *Forget Nuclear Weapons, Cutting Undersea Cables Could Decisively End a War*, NAT'L INTEREST (Dec. 30, 2019), https://nationalinterest.org/blog/buzz/forget-nuclear-weapons-cutting-undersea-cables-could-decisively-end-war-108651.

23. *CPJ Journalist Security Guide, Armed Conflict,* COMM. TO PROTECT JOURNALISTS, https://cpj.org/reports/2012/04/armed-conflict.php#5 (last visited Oct. 30, 2020).

recent internet shutdown in Yemen prevented news portals from publishing and receiving timely information from reporters.[24]

Connectivity is particularly important for banking and business. Over two billion people rely on e-commerce.[25] Globally, 52% of adults have made or received digital payments over the past year, including 44% of adults in developing countries.[26] In developed countries the percentage of people reliant on financial technology can be very high: for example, in Estonia, over 80% of the population banks via the internet.[27] But even in "countries with medium levels of connectivity, between 69-95% of businesses are already online."[28] Currently, two billion people, mostly in developing countries, rely on mobile internet banking, and this number is expected to increase further.[29] This mobile banking is vital: the World Bank reports that in a Kenyan study, access to internet mobile financing "helped reduce extreme poverty among women-headed households by 22[%]," and another study in Malawi found that internet access enabled farmers to increase crop values by 15%.[30]

B. Increasing Reliance on Internet Connectivity

Human activities will become even more connected to the internet with the advent of the 'Internet of Things.'[31] Everything from locks and doorbells to thermostats, watches, and appliances will likely need internet access to function properly.[32] Driverless, internet-reliant

---

24. Jakub Dalex et al., *Information Controls During Military Operations*, CITIZEN LAB (Oct. 21, 2015), https://citizenlab.ca/2015/10/information-controls-military-operations-yemen.

25. *Global E-Commerce Sales to Reach Almost $4 Trillion by the End of 2020*, WFMJ (Sept. 14, 2020, 9:37 AM), https://www.wfmj.com/story/42624792/global-e-commerce-sales-to-reach-almost-4-trillion-by-the-end-of-2020.

26. *The Global Findex Database 2017*, WORLD BANK, https://globalfindex.worldbank.org/basic-page-overview (last visited Oct. 30, 2020).

27. Colin Woodard, *Estonia, Where Being Wired is a Human Right*, CHRISTIAN SCI. MON. (July 1, 2003), https://www.csmonitor.com/2003/0701/p07s01-woeu.html.

28. DELOITTE CONSULTING, *supra* note 20, at 22 tbl.3.

29. Danny Parisi, *Mobile Banking to Grow to 2B Users by 2020: Report*, RETAIL DIVE, https://www.retaildive.com/ex/mobilecommercedaily/mobile-banking-to-grow-to-two-billion-users-by-2020-report (last visited Oct. 30, 2020).

30. WORLD BANK, *supra* note 26.

31. A term coined by Kevin Ashton. Tim Cole, *Interview with Kevin Ashton - Inventor of IOT: Is Driven by the Users*, SMART INDUS. (Feb. 11, 2018), https://www.smart-industry.net/interview-with-iot-inventor-kevin-ashton-iot-is-driven-by-the-users.

32. Andrew Meola, *A Look at Examples of IoT Devices and Their Business Applications in 2020*, BUS. INSIDER (Dec. 18, 2019, 12:02 PM), https://www.businessinsider.com/internet-of-things-devices-examples.

vehicles and trains are already in use.[33] In medicine, fitness bracelets, medical monitoring, heart pacemakers, insulin pumps, and remote surgical systems deliver lifesaving internet-enabled health care.[34]

Applications of internet-reliant artificial intelligence (AI), are also coming to fruition "in the next decade" and will be "embed[ded] in most human endeavors."[35] These will include specialized life-saving individualized medical diagnosis (e.g., cancer screening based on image recognition), power grids, transportation networks (e.g., driverless vehicles), disaster warning, educational delivery, logistical management, and even passive law enforcement.[36] AI has been used to monitor and predict oncoming heart attacks and strokes.[37] Corporate giant Amazon has begun operating supermarkets that rely on artificial intelligence and surveillance to monitor and charge for items taken off the shelves by customers.[38] These "networked, intelligent systems" require internet connectivity, so future generations will be more reliant on internet access than we are today.

C. Internet Connectivity Vulnerability

The internet's growth has also created vulnerabilities, both physical and digital. Actors have developed a range of different means

---

33. More than 1,400 autonomous vehicles are on the road in the U.S. Darrell Etherington, *Over 1,400 Self-Driving Vehicles Are Now in Testing by 80+ Companies Across the US*, TECHCRUNCH (June 11, 2019, 11:54 AM), https://techcrunch.com/2019/06/11/over-1400-self-driving-vehicles-are-now-in-testing-by-80-companies-across-the-u-s; Justin Franz, *How Autonomous Freight Trains Powered by Artificial Intelligence Could Come to a Railroad Near You*, SEATTLE TIMES (Mar. 10, 2020, 6:00 AM), https://www.seattletimes.com/seattle-news/how-autonomous-freight-trains-powered-by-artificial-intelligence-could-come-to-a-railroad-near-you.

34. Larry Alton, *Health vs. Hackers: Cloud-Connected Cardiac Care*, DIGITALIST (July 13, 2018), https://www.digitalistmag.com/iot/2018/07/13/health-vs-hackers-cloud-connected-cardiac-care-06178927; Ryan Madder, *Robot Surgery Could Be the Future of Health Care in Remote Areas*, FORTUNE (Feb. 11, 2020, 3:32 PM), https://fortune.com/2020/02/11/tele-robotics-surgery-5g-health.

35. Janna Anderson & Lee Rainie, *Improvements Ahead: How Humans and AI Might Evolve Together in the Next Decade*, PEW RES. CTR. (Dec. 10, 2018), https://www.pewresearch.org/internet/2018/12/10/improvements-ahead-how-humans-and-ai-might-evolve-together-in-the-next-decade (referencing Tim Morgan's description of artificial intelligence).

36. *Id.* (referencing Mícheál Ó Foghlú regarding cancer, Craig Mathias regarding systems, and Mike Osswald regarding disaster management).

37. Vanessa Chalmers, *World's First AI Can Predict When Patients Will Have a Heart Attack or Stroke Better Than a Doctor, Study Shows*, DAILY MAIL (Feb. 14, 2020, 6:47 AM), https://www.dailymail.co.uk/health/article-8003697/Worlds-AI-predict-patients-heart-attack-stroke-better-DOCTOR.html.

38. Jason Del Rey, *Amazon is Opening a Supermarket with No Cashiers. Is Whole Foods Next?*, VOX RECODE (Feb. 25, 2020, 3:01 AM), https://www.vox.com/recode/2020/2/25/21151289/new-amazon-go-grocery-store-supermarket-cashiers-whole-foods-seattle.

and methods for restricting a civilian population's ability to access the internet. For example, shutdowns, referred to as "blackouts" or "kill switches,"[39] "intentional[ly] disrupt[] . . . internet-based communications, rendering them inaccessible or effectively unavailable, for a specific population, location, or mode of access, often to exert control over the flow of information."[40]

States and other belligerents may direct shutdowns within their own borders. Usually, this entails a governmental or martial authority directing Internet Service Providers (ISPs) to stop providing routing services.[41] Blackouts can affect an entire nation or be locally targeted.[42] There has recently been a sharp uptick in internet shutdowns, particularly in response to domestic uprisings and in non-international armed conflicts (NIACs). This trend started in 2011 when the Egyptian government blocked access the internet for a week to disrupt anti-government protestors' communications.[43] In 2019, there were 213 internet shutdowns in 33 countries,[44] up from 106 in 2017 and 75 in 2016.[45] Recent examples include incidents in Ethiopia, Democratic Republic of the Congo, India, Mauritania, Myanmar, Sri Lanka, Sudan, Yemen, and Zimbabwe.[46] Shutdowns are now also clearly being used tactically in armed conflict situations, such as in Ethiopia, Myanmar, Syria, and Yemen, where the violence is protracted and opposition highly organized.[47] In 2012, Syria's government imposed a nationwide internet shutdown after previously

---

39. BERHAN TAYE ET AL., ACCESS NOW, TARGETED, CUT OFF, AND LEFT IN THE DARK: THE #KEEPITON REPORT ON INTERNET SHUTDOWNS IN 2019, at 2 (2020) [hereinafter TAYE 2019 REPORT].

40. *Policy Brief: Internet Shutdowns*, INTERNET SOC'Y (Dec. 18, 2019), https://www.internetsociety.org/policybriefs/internet-shutdowns.

41. Isabel Linzer, *An Explainer for When the Internet Goes Down: What, Who, and Why?*, FREEDOM HOUSE (July 29, 2019), https://freedomhouse.org/article/explainer-when-internet-goes-down-what-who-and-why.

42. *Id.*

43. Christopher Williams, *How Egypt Shut Down the Internet*, TELEGRAPH (Jan. 28, 2011, 11:29 AM), https://www.telegraph.co.uk/news/worldnews/africaandindianocean/egypt/8288163/How-Egypt-shut-down-the-internet.html.

44. TAYE 2019 REPORT, *supra* note 39, at 1.

45. BERHAN TAYE ET AL., ACCESS NOW, THE STATE OF INTERNET SHUTDOWNS AROUND THE WORLD:THE 2018 #KEEPITON REPORT 3 (2018).

46. TAYE 2019 REPORT, *supra* note 39, at 2-4.

47. *Id.*; Craig Timberg & Babak Dehghanpisheh, *Syria's Internet Shutdown Leaves Information Void, May Signal Escalating War*, WASH. POST (Nov. 29, 2012), https://www.washingtonpost.com/world/national-security/internet-shutdown-in-syria-sparks-panic-creates-information-void/2012/11/29/bd35a5d0-3a64-11e2-b01f-5f55b193f58f_story.html; *Internet Disrupted in Ethiopia as Conflict Breaks out in Tigray Region,* NETBLOCKS (Nov. 4, 2020), https://netblocks.org/reports/internet-disrupted-in-ethiopia-as-conflict-breaks-out-in-tigray-region-eBOQYV8Z.

imposing local blackouts in rebel-controlled areas.[48] In Yemen, in 2015, after Houthi rebels took control of the Ministry of Telecommunications and Information Technology, including the state-owned ISP, YemenNet, they "began to filter and censor various news sites, and eventually . . . shut down [access to] the internet completely, multiple times."[49] In Myanmar, during the 2019-2020 conflict between the military and the ethnic Rohingya Arakan Army, the government shutdown the mobile internet for over one million people for more than a year, complicating the provision of aid, and preventing people from becoming aware of critical public health information, including the spread of coronavirus.[50] Aid workers noted shortages of food and water in many villages and observed that digital remittances could not be transferred.[51] These instances suggest civilian internet shutdowns are becoming a common tactic in armed conflict.

In addition, shutdowns can be perpetrated by electronic attack. For example, hackers might employ a denial of service (DoS) attack to block access to websites by overwhelming a server with more requests than it can process.[52] When this type of cyber operation targets a Domain Name System (DNS) server, which acts as the internet's directory of web addresses, millions of people can be effectively denied access to websites. This occurred most notoriously in the U.S. in 2016, when the Mirai botnet denied access to the Dyn, a major domain name system, taking much of the eastern U.S. offline.[53] In 2007, Russia-affiliated hackers used a distributed DoS attack against Estonia to shut down banking, government services, and

48. Martin Chulov, *Syria Shuts Off Internet Access Across the Country*, THE GUARDIAN (Nov. 29, 2012, 12:30 PM), https://www.theguardian.com/world/2012/nov/29/syria-blocks-internet.

49. Emna Sayadi & Berhan Taye, *#KeepItOn: As Yemen's War Goes Online, Internet Shutdowns and Censorship Are Hurting Yemenis*, ACCESS NOW (Jun. 25, 2020 2:35 PM), https://www.accessnow.org/keepiton-as-yemens-war-goes-online-internet-shutdowns-and-censorship-are-hurting-yemenis; Jakub Dalek et. al, *Information Controls During Military Operations: The Case of Yemen During the 2015 Political Armed Conflict*, CITIZEN LAB (Oct. 21, 2015), https://citizenlab.ca/2015/10/information-controls-military-operations-yemen.

50. *Myanmar: End World's Longest Internet Shutdown*, HUM. RTS. WATCH (June 19, 2020, 8:00 AM), https://www.hrw.org/news/2020/06/19/myanmar-end-worlds-longest-internet-shutdown.

51. *Id.*

52. This is usually conducted using pre-programmed code ('bot') which is set to access a site at a specific time; when a large number of such bots (a 'bot army') make the requests at the same time, the server cannot process the information and legitimate traffic is essentially blocked from accessing the particular site.

53. Nicky Woolf, *DDoS Attack That Disrupted Internet Was Largest of its Kind in History, Experts Say,* THE GUARDIAN (Oct. 26, 2016, 9:42 PM), https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet; Lily Hay Newman, *What We Know About Friday's Massive East Coast Internet Outage,* WIRED (Oct. 21, 2016), https://www.wired.com/2016/10/internet-outage-ddos-dns-dyn.

media sites.[54] Though these DDoS operations occurred outside of armed conflict, it is easy to see how the tactic could similarly be employed during wartime to harass and terrorize the civilian population.

Civilian internet access can also be severed by physical destruction. The internet's cyber realm manifests in physical space as servers, data processors, and transmission cables. Destroying or degrading this equipment could prevent civilian internet access during armed conflict. The most vulnerable link appears to be transmission cables, on which 99% of international internet data is sent.[55] These can be easily cut,[56] and the damage to a single communication cable could impact a tremendous number of civilians. For example, in 2018, Houthi-rebels cut Yemen's main fiber optic cable in three locations, severing internet access for 80% of the population.[57] If a major cable across the Atlantic were cut, ordinary users in the U.S. would experience tremendous losses of bandwidth and potentially be cut off from data, as key digital service providers, like Google and Facebook, store users' electronic data in overseas servers.[58] The United Nations recognized these internet cables as "vitally important to the global economy and the national security of all states,"[59] especially international trade, with over $10 trillion transferred each

54. Damien McGuinness, *How A Cyber Attack Transformed Estonia*, BBC (Apr. 27, 2017), https://www.bbc.com/news/39655415.

55. Douglas Main, *Undersea Cables Transport 99 Percent of International Data*, NEWSWEEK (Apr. 2, 2015, 12:39 PM), https://www.newsweek.com/undersea-cables-transport-99-percent-international-communications-319072.

56. U.S. OFFICE OF THE DIR. OF NAT'L INTELLIGENCE & U.S. DEP'T OF HOMELAND SEC., THREATS TO UNDERSEA CABLE COMMUNICATIONS 13-14, 22 (2017); *see also* NATO COOP. CYBER DEF. CTR. OF EXCELLENCE, STRATEGIC IMPORTANCE OF, AND DEPENDENCE ON UNDERSEA CABLES (2019)..

57. Ali Mahmood, *Houthis Cut Off Internet to 80 Per Cent of Yemen*, THE NAT'L (Jul. 5, 2018, 10:13 PM), https://www.thenationalnews.com/world/mena/houthis-cut-off-internet-to-80-per-cent-of-yemen-1.747535.

58. Garrett Hinck, *Evaluating the Russian Threat to Undersea Cables*, LAWFARE (Mar. 5, 2018, 7:00 AM), https://www.lawfareblog.com/evaluating-russian-threat-undersea-cables; *see also* Andrew K. Woods, *Against Data Exceptionalism*, 68 STAN. L. REV. 729, 739 (2016) ("[O]ne of the greatest societal and technological shifts in recent years has been the move from storing data on a local machine—such as a cell phone or computer—to storing that data remotely on faraway servers, which can be accessed by a network such as the Internet."); AWS, AMAZON WEB SERVICES POLICY PERSPECTIVES: DATA RESIDENCY (2020)(arguing that Amazon should not be limited to storing American user data in the United States); Guoxin Liu & Haiying Shen, *Minimum-Cost Cloud Storage Service Across Multiple Cloud Providers*, *in* 2016 IEEE 36TH INTERNATIONAL CONFERENCE ON DISTRIBUTED COMPUTING SYSTEMS (ICDCS) 129 (2016) (observing service providers shift data to the lowest costs data center around the world).

59. G.A. Res. 65/37, at 3 (Mar. 17, 2011).

day.[60] These cables also carry sensitive diplomatic and military communications.[61]

Among transmission cables, undersea cables, often considered the 'internet's backbone,' are particularly vulnerable.[62] Bryan Clark, a senior naval strategist, reveals that "there are a lot of countries and companies that have the ability to send vehicles down to the seafloor and have them manipulate . . . or take away undersea cables."[63] In 2013, a saboteur diver cut part of the SEA-ME-WE-4 fiberoptic cable, which carries the majority of electronic data between southeast Asia, south Asia, the Middle East, and North Africa to western Europe, reducing Egypt's internet bandwidth by 60%.[64] In 2015, the U.S. found that Russia's high-tech *Yantar* ship was carrying deep-sea submersibles and cable-cutting gear over the North Atlantic submarine cables.[65] According to former NATO Submarine Commander U.S. Rear Admiral Andrew Lennon, "we are now seeing Russian underwater activity in the vicinity of undersea cables that I don't believe we have ever seen."[66] Major powers appear to be preparing to attack or defend internet connectivity, thus underscoring the risk and illustrating the impetus to address these concerns with international legal safeguards.

These examples illustrate the increasing importance of internet connectivity to civilians, while also highlighting threats and

---

60. Tim Johnson, *Undersea Cables: Too Valuable to Leave Vulnerable*, GOV'T TECH. (Dec. 12, 2017), https://www.govtech.com/network/Undersea-Cables-Too-Valuable-to-Leave-Vulnerable.html.

61. Hinck, *supra* note 58.

62. Matt Blitz, *How Secret Underwater Wiretapping Helped End the Cold War*, POPULAR MECH.'S (Mar. 20, 2017), https://www.popularmechanics.com/technology/security/a25857/operation-ivy-bells-underwater-wiretapping (quoting former U.S. Navy submariner Craig Reed); *see also* Nadia Schadlow & Brayden Helwig, *Protecting Undersea Cables Must Be Made A National Security Priority*, DEF. NEWS (July 1, 2020), https://www.defensenews.com/opinion/commentary/2020/07/01/protecting-undersea-cables-must-be-made-a-national-security-priority.

63. Johnson, *supra* note 60. (quoting Bryan Clark, a naval strategist at the Center for Strategic and Budgetary Assessments).

64. Bryan Clark, *Undersea Cables and the Future of Submarine Competition*, 72 BULL. ATOMIC SCIENTISTS 234, 235-236 (2016), *see also* Amanda Williams, *Three Egyptian Divers 'Tried to Hack Through Internet Ocean-Floor Cables in Attack that Could Have Taken Entire Continent Offline'*, DAILY MAIL (Mar. 28, 2013, 5:19 PM), https://www.dailymail.co.uk/sciencetech/article-2300595/Pictured-Egyptian-divers-tried-hack-cables-attack-crashed-internet-worldwide.html. Egypt has not disclosed who the divers were or whether they were prosecuted.

65. Johnson, *supra* note 60.

66. Pete Barker, *Undersea Cables and the Challenges of Protecting Seabed Lines of Communication,* CTR. FOR INT'L MAR. SEC. (Mar. 15, 2018), http://cimsec.org/undersea-cables-challenges-protecting-seabed-lines-communication/35889.

vulnerabilities, including shutdowns, electronic attacks, or destruction of physical infrastructure. This underscores the importance of clearly articulating and protecting the right to access the internet in the international legal system.

III. PROTECTIONS FOR INTERNET ACCESS UNDER INTERNATIONAL LAW

Protections for internet access during armed conflict derive from human rights law, humanitarian law (also known as the law of armed conflict, or LOAC), international communications systems law, and law governing submarine cables. Yet, as the following discussion illustrates, none of these systems of international rules and norms, individually or collectively, function to provide adequate protections during armed conflict. International human rights law (IHRL) provides seemingly strong protections for civilian internet access as a basic right, but ill-defined exceptions for emergencies, and ambiguity regarding its applicability to conflict situations, undermine the regime's effectiveness. Under LOAC, civilian internet access does not enjoy special protections, and traditional principles leave civilian internet access vulnerable to a range of possible interpretations of what legal safeguards should apply during armed conflict. Similarly, telecommunications and antiquated undersea cable protection law are inadequate to protect the internet infrastructure so vital to contemporary global society.

As a preliminary matter, it is important to note the unique nature of harms caused by the denial of internet access, which distinguish it from other 'cyber harms,' motivating the need for special protective international frameworks. "[H]arms committed in [the cyber realm] are often dismissed as 'not really real,' as they are by their nature not physical, bodily harms . . . and thus should not be taken very seriously."[67] One may question whether the mere invasion of a network, deletion of files, or alteration of code truly constitutes a harm recognizable under international law. Loss of civilian internet access is entirely different: the harm to the civilian is immediately manifest in the deprivation of civilians' ability to acquire information and communicate with the modern world. The deprivation of internet access may conceivably cause immediate physical harm, for instance the loss of connectivity to remotely-controlled medical devices and vehicles.[68] Moreover, the second- and third-order effects,

67. Mary Anne Franks, *Unwilling Avatars: Idealism and Discrimination in Cyberspace*, 20 COLUM. J. GENDER L. 224, 255-56 (2011).

68. *See e.g.*, Mitch Koczerginski, *The Cybersecurity Implications of Driverless Cars*, CYBERSEC. BULL. (Dec. 2016), https://www.mcmillan.ca/The-Cybersecurity-Implications-of-Driverless-Cars ("Driverless cars must also be able to interact and exchange data with one another in real time."); Andrew Steger, *How the Internet of Medical Things Is Impacting Healthcare*, HEALTHTECH (Jan. 16,

along with repercussive and reverberating effects of severed internet access, can cause serious and lasting harm to a civilian population. For example, the inability to order food, adequately stock medications, access electronic funds, or efficiently conduct business could clearly result in significant humanitarian harm, as discussed in Section I. However, even when disabling internet access causes no immediate physical harm, it infringes upon a more basic right to connect, which has motivated IHRL protection and should warrant recognition under LOAC.

A. International Human Rights Law (IHRL) Protection

The global community has long recognized the importance of internet connectivity to modern society. During the 2003 United Nations World Summit on the Information Society, delegates "reaffirm[ed] as an essential foundation of Information Society . . . [the Universal Declaration of Human Rights mandate] that everyone has the right to freedom of opinion and expression. . . . Communication is a fundamental social process, a basic human need and the foundation of all social organization."[69] Similarly, as noted above, much of the global public considers access to the internet a basic right.[70] Ethicists credit the internet with providing "freedom, justice, and safety to marginalized groups," pointing to coronavirus citizen journalists, the Arab Spring, the #MeToo campaign, and attempts to document police brutality around the world as examples.[71]

2020), https://healthtechmagazine.net/article/2020/01/how-internet-medical-things-impacting-healthcare-perfcon (continuously connected devices are playing a "central part in tracking and preventing chronic illnesses.").

69. World Summit on Information Society, *Declaration of Principles*, WSIS-03/Geneva/Doc/4-E (Dec. 12, 2003)., 1 (referencing Universal Declaration of Human Rights, at Art. 19). The nature of this right is disputed. While there is almost universal agreement that access to the internet should not be blocked, some go further arguing access to the internet itself is an affirmative right which should be provided to all free of charge. Some governments subsidize universal internet access, i.e. the European Union's WiFi4EU initiative, Estonia, Finland, Spain, and Kerala, India. *See* Stephanie Borg Psaila, *Right to Access the Internet: the Countries and the Laws That Proclaim it*, DIPLO (May 2, 2011), https://www.diplomacy.edu/blog/right-access-internet-countries-and-laws-proclaim-it; *WiFi4EU: Free Wi-fi for Europeans*, EUR. COMMISSION, https://ec.europa.eu/digital-single-market/en/wifi4eu-free-wi-fi-europeans (last visited Feb. 6, 2020); *Recognise the Internet as a Human Right, Says Sir Tim Berners-Lee as he Launches Annual Web Index*, WORLD WIDE WEB FOUND. (Dec. 10, 2014), https://webfoundation.org/2014/12/recognise-the-internet-as-a-human-right-says-sir-tim-berners-lee-as-he-launches-annual-web-index.

70. INTERNET SOC'Y, *supra* note 17.

71. David Nield, *Should Free Internet Be A Basic Human Right? There's a Strong Case for It*, SCI. ALERT (Nov. 12, 2019), https://www.sciencealert.com/here-s-why-one-scientist-believes-free-internet-should-be-a-basic-human-right.

While there is still some philosophical debate among experts,[72] IHRL has largely recognized the importance of internet access as an integral human right.

Article 19 of the International Covenant on Civil and Political Rights (ICCPR), a multilateral treaty with 173 states parties including the U.S.,[73] declares that "everyone shall have right[s]: to hold opinions without interference . . . freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers . . . through any . . . media of his choice."[74] The U.N. Human Rights Committee, the UN a treaty-monitoring body for the ICCPR, issued interpretative guidance stating Article 19 of the ICCPR protects the means by which all forms of expression are disseminated, including "electronic and internet-based modes of expression."[75] Scholars, diplomats, policymakers and human rights advocates similarly assert that Article 19 clearly guarantees a right to internet access. Most prominently, Frank Rue, the U.N. Special Rapporteur on the Protection of the Right to Freedom of Opinion and Expression, issued a report to the U.N. Human Rights Council in 2011 in which he noted "the right of all individuals to seek and receive and impart information and ideas of all kinds of media" includes "the internet [which] has become an

72. Vinton Cerf, *Internet Access is Not a Human Right*, N.Y. TIMES (Jan. 4, 2012), https://www.nytimes.com/2012/01/05/opinion/internet-access-is-not-a-human-right.html (The author, an internet pioneer, claims that "technology is an enabler of rights, not a right itself" and argues that freedom of speech or access to information should be protected rather than "a specific piece of technology."); Brian Skepys, *Is There A Human Right to the Internet*, 5 J. POL. & L.15 (2012) (arguing only "instrumentally necessary things for membership in a political community" should be considered human rights and to him internet access is "valuable" but not necessary.); Sherif Elsayed-Ali, *Internet Access is Integral to Human Rights*, EGYPT INDEP. (Jan. 15, 2012, 1:31 PM), https://egyptindependent.com/internet-access-integral-human-rights (explaining that "the rights to freedom of speech and freedom of access to information would be meaningless if they did not protect the means of enjoying them. . . . by today's standards [people deprived on internet access would] be cut off from the outside world . . . [p]olitical news, scientific discoveries and public health advice would be slow to reach the country and spread to the population. . . . The economy, education, science and cultural life would suffer.").

73. As of March 2020, there were 173 parties. *International Covenant on Civil and Political Rights: Status*, U.N. TREATY COLLECTION, https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-4&chapter=4&clang=_en (last visited Nov. 25, 2020).

74. International Covenant on Civil and Political Rights, art. 19, Dec. 16, 1966, 999 U.N.T.S. 171.

75. U.N. Human Rights Comm., International Covenant on Civil and Political Rights, ¶ 11, U.N. Doc. CCPR/C/GC/34 (Sept. 12, 2011), ("States parties [must] guarantee the right to freedom of expression, including the right to seek, receive and impart information and ideas of all kinds regardless of frontiers.... [including] communications of every form of idea and opinion capable of transmission to others... [and] protects . . . the means of their dissemination.... [including] electronic and internet-based modes of expression.").

indispensable tool."[76] The U.N. Human Rights Council followed suit in 2016, declaring unfettered internet access protected under the "right to freedom of opinion and expression."[77]

Prominent judicial institutions around the world have likewise recognized the right of citizens not to be deprived of access to the internet. In 2017, the United States Supreme Court unanimously struck down a state law prohibiting convicted sex offenders from accessing social media websites.[78] Justice Kennedy, writing for the majority, explained a government cannot "bar[] access to what for many are the principal sources for knowing current events, checking ads for employment, speaking and listening in the modern public square, and otherwise exploring the vast realms of human thought and knowledge."[79] Similarly, a French law suspending internet access to persons who illegally downloaded files was found unconstitutional as it impacted fundamental rights without adequate due process.[80] In 2015, the European Court of Human Rights likewise recognized a right to internet access, which had "become one of the main means by which individuals could exercise their right to freedom to receive and impart information and ideas."[81] This domestic recognition of a right not to be deprived of internet access reflects an international trend.

Under IHRL, the human right to access the internet exists at all times, including during war, and can only be abrogated in exceptional circumstances. The ICCPR permits derogation of protected rights only in "time of public emergency which threatens the life of the

---

76. Frank La Rue (Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression), *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression,*, ¶ 67, U.N. Doc A/HRC/17/27 (May 16, 2011) ("the Internet boosts economic, social and political development, and contributes to the progress of humankind as a whole").

77. The Human Rights Council explained internet access is "one of the most powerful instruments of the 21st century for increasing transparency in the conduct of the powerful, access to information, and for facilitating active citizen participation in building democratic societies." Bode, *supra* note 18.

78. Packingham v. North Carolina, 137 S. Ct. 1730, 1737 (2017).

79. *Id.* at 1732. But, in concurrence Justice Alito contemplated situations where limited restrictions to internet access might be permissible such as blocking specific websites to protect children. *Id.* (Alito J, concurring).

80. *French Court Curbs Disputed Internet Piracy Rules*, REUTERS (June 10, 2009), https://in.reuters.com/article/oukin-uk-france-internet/french-court-curbs-disputed-internet-piracy-rules-idUKTRE5596CO20090610. The French Digital Minister arguing that the law should have been overturned, observed "[i]n this day and age it's not possible to cut off someone's Internet access. It's like cutting off their water." *France 'Cuts Off' Illegal Downloader's Web Access*, FRANCE24 (June 14, 2014), https://www.france24.com/en/20130614-french-downloader-first-have-web-access-cut-off.

81. Cengiz & Others v. Turkey, App. Nos. 48226/10 and 14027/11, Eur. Ct. H.R. § 38 (2015)

nation."[82] However, the basis for invoking a 'public emergency' is limited. The ICJ ruled that "the protection under the [ICCPR] does not cease in times of war, except [when] certain provisions may be derogated from in a time of national emergency."[83] The U.N. Human Rights Committee (UNHCR), an independent panel of experts charged with monitoring the implementation of the ICCPR among states parties, opines "even during an armed conflict measures derogating from the [ICCPR] are allowed only if and to the extent that the situation constitutes a threat to the life of the nation."[84] Thus, the human right to internet access should legally apply during wartime in both international and non-international armed conflicts unless the 'life of the nation' is threatened. Echoing the ICJ and UNHCR's sentiment of universal application, U.N. Special Rapporteur Frank La Rue "call[ed] upon all States to ensure that Internet access is maintained at all times" and "consider[ed] cutting off users from Internet access, regardless of the justification . . . to be disproportionate and thus a violation of Article 19, paragraph 3, of the [ICCPR]."[85] La Rue explained there should be "as little restriction as possible to the flow of information via the Internet, except in a few, exceptional, and limited circumstances prescribed by international human rights law." Additionally, any restriction must be clearly provided by law, must be proven to be necessary, and must be the least intrusive means available.[86] Thus, La Rue applied the broad protections of the ICCPR, recognized by the ICJ, to internet access, though he acknowledges that it could still be overridden in extreme circumstances. Though some armed conflicts do not threatened the 'life of the nation,' e.g. a superpower's involvement in war against insurgent groups in a distant country, many armed conflicts could be categorized as 'threatening the life of the nation' such that the protections for internet access derived from the ICCPR might be circumvented.

Additionally, the geographic applicability of the ICCPR remains subject to disagreement. The U.N. Human Rights Committee says the ICCPR applies extraterritorially.[87] Yet not all states parties accept

---

82. International Covenant on Civil and Political Rights, *supra* note 74, at art. 4(1).

83. Legality of the Threat or Use of Nuclear Weapons (United Nations), Advisory Opinion, 1996 I.C.J. 226, 240 (July 8, 1996) [hereinafter Legality of the Threat or Use of Nuclear Weapons].

84. U.N. Human Rights Comm., General Comment on Article 4, para. 3, U.N. Doc. CCPR/C/21/Rev.1/Add.11 (July 24, 2001).

85. La Rue, *supra* note 76 (applying ICCPR arts. 78 & 79).

86. *Id.* at ¶ 68.

87. U.N. Human Rights Comm., *Concluding Observations on the Fourth Report of the United States of America*, U.N. Doc. CCPR/C/USA/CO/4 (2014) (finding the United States, an ICCPR member had an obligation to respect ICCPR protections and apply them to non-residents abroad with respect to privacy from state surveillance); Frank La Rue, *supra* note 76, at ¶¶ 24(c), 31, 49.

extraterritorial jurisdiction. For example, the U.S. disputes extraterritorial jurisdiction, arguing that the ICCPR was intended only to apply domestically to physical places under the "effective control" of the states parties.[88] Others disagree, claiming the ICCPR applies extraterritorially when states parties have "control over a particular person or context," such as when a government conducts phone tapping surveillance abroad.[89] This disagreement has significant relevance to armed conflict, where invading states could claim the ICCPR does not apply because they do not have absolute control over a territory. These disputes related to emergency situations and extraterritorial applicability illustrate important potential limitations on the extent of the ICCPR's protection for civilian internet access.

B. Law of Armed Conflict (LOAC) Protection

1. LOAC Offers General and Provisional Protection for Civilian Internet Connectivity

No current LOAC provisions specifically provide for or explicitly protect internet access. However, the generally applicable provisions of LOAC covering civilian objects provide some limited and conditional protection. For example, during hostilities, the belligerents' right "to choose methods or means of warfare is not unlimited."[90] Furthermore, the time-honored rules and principles of the LOAC—necessity, distinction, proportionality, and humanity—create a framework aiming to avoid unnecessary harm, especially to civilians.

One seemingly powerful source of protection stems from LOAC's general bar against belligerents attacking civilian objects. The 1977 Additional Protocol to the Geneva Conventions (Additional Protocol I) mandates that "attacks shall be limited strictly to military objectives."[91] Valid military objectives are those which, by their

88. *See Testimony of John B. Bellinger III*, JUST SEC. (Mar. 19, 2014), https://www.justsecurity.org/wp-content/uploads/2014/03/Bellinger_PCLOB_comment_3-17-14.pdf (posting the testimony of the former Legal Adviser for the Department of State before the Privacy and Civil Liberties Oversight Board (PCLOB)).

89. Martin Scheinin, *Letter to the Editor from Former Member of the Human Rights Committee*, JUST SEC. (Mar. 10, 2014), https://www.justsecurity.org/8049/letter-editor-martin-scheinin/ (quoting Harold Koh).

90. Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), art. 35(1), June 8, 1977, 1125 U.N.T.S. 3 [hereinafter Additional Protocol I]. This is a long-established principle understood through customary international law. *See, e.g.*, Convention on the Law and Customs of War on Land (Hague IV), reg. art. 22, October 18, 1907.

91. *Id.*

"nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage."[92] Furthermore, "[belligerents] shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives . . . direct[ing] their operations *only against military objectives*."[93] This principle of 'distinction' is considered customary international law (CIL) and followed even by non-signatories to Additional Protocol I, including the U.S.[94] Similarly, LOAC generally prohibits 'indiscriminate attacks' which are not directed at a specific military objective, but "strike military objectives and civilians or civilian objects without distinction."[95] The International Court of Justice (ICJ) has likewise stressed the importance of protecting civilian objects, recognizing certain "cardinal" principles of armed conflict: "never mak[e] civilians the object of attack" and "never us[e] weapons that are incapable of distinguishing between civilian and military targets."[96]

However, under LOAC, protection of civilian objects such as infrastructure is not absolute, but is balanced against military objectives under the principle of 'proportionality.' Article 57 of Additional Protocol I mandates that states parties "refrain from deciding to launch any attack which may be expected to cause . . . damage to civilian objects, or a combination thereof, which would be *excessive in relation* to the concrete and direct military advantage anticipated."[97] Accordingly, LOAC also generally permits civilian objects to be the subject of attack, if warranted by military necessity. As will be discussed in greater detail below in Part III, these qualifications and other ambiguities render protections inadequate. In these ways, LOAC differs sharply from the clear protections of

92. *Id.*

93. *Id.* at art. 48 (emphasis added).

94. *See, e.g., Practice Relating to Rule 1. The Principle of Distinction between Civilians and Combatants,* INT'L COMM. OF THE RED CROSS: IHL DATABASE*,* https://ihl-databases.icrc.org/customary-ihl/eng/docs/v2_rul_rule1_sectiona (last visited Apr. 4, 2020).

95. Additional Protocol I, *supra* note 90, at art. 51(4). 174 States were party as of March 2020, but the United States, Pakistan, and Iran signed but have not ratified. For a list of states parties *see*, *Treaties, States Parties and Commentaries: Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977*, INT'L COMM. OF THE RED CROSS: IHL DATABASE, https://ihl-databases.icrc.org/ihl/INTRO/470 (last visited Mar. 1, 2020); *see also* Michael J. Matheson, *The United States Position on the Relation of Customary International Law to the 1977 Protocols Additional to the 1949 Geneva Conventions*, 2 AMER. U. J. INT'L L. & POL'Y 419 (1987).

96. Legality of the Threat or Use of Nuclear Weapons, *supra* note 83, at 257.

97. Additional Protocol I, *supra* note 90, at art. 57(2)(a)(iii) (emphasis added)).

human rights law, thus raising the question of whether IHRL of LOAC applies.

2. LOAC applies *Lex Specialis* during Armed Conflict, but IHRL Principles Still Apply

Human rights law more clearly provides protections for internet access than LOAC. But how much, if any, human rights law should apply during an armed conflict, especially when it differs from LOAC? Scholars and states disagree over how IHRL and LOAC should interact, with some suggesting each body of law should apply exclusively and others arguing for a complementary, mutually reinforcing interpretation, which would apply both simultaneously. While there has been a "growing trend [towards applying IHRL to conflicts] which comes with an exponential explosion of jurisprudence and academic legal literature on this subject,"[98] traditionally, LOAC is generally thought to override IHRL in the context of armed conflict under cannons for interpreting international law, such as the doctrine of *lex specialis*.

With respect to the ICCPR, historic canons and ICJ jurisprudence largely resolve the matter. Historically, LOAC has always been considered to override other laws and norms during armed conflict, under the doctrine of *lex specialis*.[99] This doctrine of international law holds that when equally applicable laws conflict, interpretive deference should be given to the one which is more specific.[100] Thus, when contextually activated the laws of war function as "*leges speciales* [special legislation] in relation to—and thus override—rules laying out the peace-time norms relating to the same subjects."[101] Later, the ICJ held that LOAC applies *lex specialis*, specifically governing the conduct of parties during times of armed conflict.[102] In a case involving the right to life in wartime, when asked whether the ICCPR or LOAC should apply, an ICJ advisory opinion held that the "test of what is an arbitrary deprivation of life . . . [should]

---

98. Ezequiel Heffes, *Book Review: Gerd Oberleitner, Human Rights in Armed Conflict: Law, Practice, Policy (Cambridge University Press, Cambridge, 2015)*, 97 INT'L REV. RED CROSS 929, 929 (2015). Now, many organizations, including the International Committee of the Red Cross, assert "[IHRL] is applicable in all situations." Marco Sassòli et al. *IHL and Human Rights,* INT'L COMM. OF THE RED CROSS, https://casebook.icrc.org/law/ihl-and-human-rights (last visited a Nov. 21, 2020).

99. Legality of the Threat or Use of Nuclear Weapons, *supra* note 83, at 240.

100. Martti Koskenniemi, Int'l Law Comm'n, *Fragmentation of International Law: Difficulties Arising from the Diversification and Expansion of International Law*, U.N. Doc. A/CN.4/L.682 (Apr. 13, 2006).

101. Heike Krieger, *A Conflict of Norms: The Relationship Between Humanitarian Law and Human Rights Law in the ICRC Customary Law Study*, 11 J. CONFLICT & SECURITY L. 265, 270 (2006).

102. Legality of the Threat or Use of Nuclear Weapons, *supra* note 83, at 240.

be determined by the applicable *lex specialis*, namely, the law applicable in armed conflict which is designed to regulate the conduct of hostilities."[103] Consequently, while the ICCPR remains in effect, the legality of attacking the internet during armed conflict would seem to be determined through LOAC analysis.

However, this is not the end of the analysis, particularly because LOAC does not provide any explicit protections for civilian internet access. LOAC has adopted much of IHRL as a matter of customary international law or as an interpretive aid, so the ICCPR may still carry weight under this analysis. For example, the Martens Clause, a provision found in many LOAC conventions such as the Geneva Conventions, stipulates that:

> in cases not covered by [IHL] conventions, neither combatants nor civilians find themselves completely deprived of protection. Instead, in such cases, the conduct of belligerents remains regulated by the principles of the law of nations as they result from the usages of international law, from the laws of humanity, and from the dictates of public conscience.[104]

Jurists often use the Martens Clause as an interpretative tool through which LOAC can reference IHRL to fill gaps not explicitly covered by the LOAC.[105] Under this approach, objects related to the provision of civilian internet access might warrant great protection under LOAC than ordinary civilian objects, because of the significant protection and special status they enjoy under IHRL derived from the ICCPR. However, IHRL protection cannot be considered absolute under LOAC, because of the deference given to military commanders in determining military necessity and proportionality when considering operations that might damage civilian objects. Thus, military commanders should consider the special importance of internet access enunciated in IHRL while conducting their traditional LOAC analysis to ensure consistency with international law, notions of humanity, and public conscience. Nonetheless, due to the Martens Clause's limited operative effect, the full import of IHRL will be significantly diluted or subsumed by other considerations as military commanders enjoy great leeway in their consideration of LOAC principles.

---

103. *Id.*

104. Vaios Koutroulis, *Martens Clause,* OXFORD BIBLIOGRAPHIES (Aug. 16, 2017), https://www.oxfordbibliographies.com/view/document/obo-9780199796953/obo-9780199796953-0101.xml.

105. Jochen von Bernstorff, *Martens Clause, in* THE MAX PLANCK ENCYCLOPEDIA OF PUBLIC INTERNATIONAL LAW 1143-46 (Rüdiger Wolfrum, ed., 2012).

3. Basic Humanitarian Principles in Non-International Armed Conflicts

There is also tension (and confusion) within LOAC regarding the applicability of provisions originally intended for international armed conflict (i.e., between states) to non-international armed conflicts (e.g., insurgencies, succession movements, etc.) Textually, the broad protections of original Geneva Conventions only apply to international armed conflicts.[106] The only protections offered in non-international armed conflicts were a right to be treated "humanely," though this right is qualified in the text by egregious examples, such as "violence to life," cruel treatment, torture, and outrages upon personal dignity.[107] Importantly, this tension affects the right to access the internet. Provisions related to civilian objects and internet access in Additional Protocol I technically and textually apply only to *international* armed conflict situations.[108] But a movement within the law seeks to more broadly apply such rules to non-international armed conflict situations as a matter of customary international law. In a non-binding 1968 resolution, the U.N. General Assembly observed "the necessity of applying basic humanitarian principles in all conflicts."[109] Similarly, the ICJ observed that certain "elementary considerations of humanity" are applicable regardless of type of armed conflict.[110] Given the broad impact of internet disruptions on the population, connectivity may be considered a basic modern consideration of humanity. Likewise, the International Criminal Tribunal of Yugoslavia noted that the "distinction [between international and non-international armed conflict] has become more and more blurred, and international legal rules have increasingly emerged or have been agreed upon to regulate internal armed

---

106. *See* Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, art. 2, Aug. 12, 1949, 6 U.S.T. 3114, 75 U.N.T.S. 31 [hereinafter First Geneva Convention]; Geneva Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea, art. 2, Aug. 12, 1949, 6 U.S.T. 3217, 75 U.N.T.S. 85 [hereinafter Second Geneva Convention]; Geneva Convention Relative to the Protection of Civilian Persons in Time of War, art. 2, Aug. 12, 1949, 6 U.S.T. 3516, 75 U.N.T.S. 287 [hereinafter Fourth Geneva Convention].

107. Common article 3 in all the original, aforementioned conventions. First Geneva Convention, *supra* note 106, at art. 3; Geneva Convention Relative to the Treatment of Prisoners of War, art. 3, Aug. 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135 [hereinafter Third Geneva Convention]; Fourth Geneva Convention, *supra* note 106, at art. 3.

108. Additional Protocol I, *supra* note 90, at art. 3.

109. G.A. Res. 2444 (XXIII), at 50 (Dec. 19, 1968).

110. *See* Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. Rep. 14, ¶ 215 (June 27) [hereinafter Military and Paramilitary Activities].

conflict."[111] A 2005 study by the International Committee of the Red Cross found that, in state practice, many international armed conflict rules have become applicable to non-international armed conflict situations.[112]While the law in this area seems to be moving toward incorporating fundamental humanitarian protections from international to non-international armed conflict, it remains unsettled. Not being able to apply the broad protections of the Geneva Conventions and Additional Protocols in situations of non-international armed conflict make it even more difficult to assert clear protections for civilian internet access under the LOAC.

C. International Communications Law Protection

International communications law poorly protects civilian internet access. The Constitution and Convention of the International Telecommunications Union (ITU), which has over 193 member states including the U.S., governs telegram, telephone, and radio communications.[113] The ITU Constitution notes that states parties cannot "cause harmful interference" with communications, but does allow exemptions, including "entire freedom with regard to military" transmissions.[114] Still, military forces "so far as possible" are obligated to refrain from interfering with civilian communications.[115] Nevertheless, this provision is weak and some military legal advisors suggest it would not even apply in an armed conflict.[116] Under the ITU Constitution, states parties can "stop the transmission of any private telegram which may appear dangerous to the security of the State or contrary to their laws, [or] to public order" and can "cut off any other private telecommunications which may appear dangerous" with a right "to suspend the international telecommunication service."[117] Although enacted before internet use became ubiquitous, the ITU Constitution remains in effect today. Troublingly, it provides almost no protections for assuring internet connectivity and instead grants to

---

111. *Prosecutor v. Tadić, Case No. IT-94-1-I,* Decision on Defence Motion for Interlocutory Appeal on Jurisdiction, ¶ 97 (Int'l Crim. Trib. for the Former Yugoslavia Oct. 2, 1995).

112. *See* JEAN-MARIE HENCKAERTS & LOUISE DOSWALD-BECK, 1 CUSTOMARY INTERNATIONAL HUMANITARIAN LAW, at xxix (2005) ("This study provides evidence that . . . State practice has gone beyond existing treaty law and expanded the rules applicable to non-international armed conflicts.").

113. Constitution of the International Telecommunication Union, Dec. 22, 1992, 1825 U.N.T.S. 331 [hereinafter ITU Constitution].

114. *Id.* at art. 45, 48 (agreeing not to cause harmful interference and granting entire freedom for national defense services).

115. *Id.* at art 48.

116. Dep't of Defense Office of Gen. Council, *An Assessment of International Legal Issues in Information Operations*, *in* 76 INT'L LEGAL STUDIES 459, 500 (1999) ("The treaty does not specifically state how--if at all-- it will apply during an armed conflict.");

117. ITU Constitution arts. 34-35.

states virtually unfettered discretion to cut access to communication which appears dangerous. Thus, the ITU Constitution fails to meaningfully safeguard civilian internet access, especially during armed conflict.

D. Antiquated Protections for Undersea Communication Cables

The legal regime protecting the internet's backbone is outdated and provides little legal protection under international law, especially during conflict. While the 1884 Convention for the Protection of Submarine Telegraph Cables technically prohibits "break[ing] or injur[ing] a submarine cable, willfully or by culpable negligence, in such manner as might interrupt or obstruct telegraphic communications" during peacetime,[118] the 136-year-old treaty merely requires states parties to adopt domestic criminal legislation protecting cables, and imposes financial responsibility for damages.[119] Importantly, the Convention does not attempt to regulate state activities or impose state responsibility during armed conflict, nor does it contemplate nefarious actions that could be conducted through or against the cables.[120]

This leaves a critical gap in protection for communications cables during wartime, which has already been abused. During World War I, the British cut undersea cables connecting Germany to the global telegraph system, redirecting 80 million German war messages through British telegram link stations in Cairo, Cape Town, Gibraltar, and Zanzibar, where they were intercepted and deciphered.[121] Today, the impact of an attack involving submarine cables could be much more devastating, especially for civilians, who are more even more dependent on the cables. Mark Sedwill, a former United Kingdom national security advisor, observed that one "can achieve the same

---

118. Convention for the Protection of Submarine Telegraph Cables, art. II, Mar. 14, 1884, 24 Stat. 989, T.S. No. 380

119. *Id.* at arts. II & XII; Tara Davenport, *Submarine Cables, Cybersecurity and International Law: An Intersectional Analysis*, 24 CATH. U. J. L. & TECH. 57, 67 (2015).

120. Tamsin P. Paige et. al, *The Final Frontier of Cyberspace: Ensuring that Submarine Data Cables are Able to Live Long and Prosper (Part I)*, OPINIO JURIS (Oct. 16, 2020), https://opiniojuris.org/2020/10/16/the-final-frontier-of-cyberspace-ensuring-that-submarine-data-cables-are-able-to-live-long-and-prosper-part-i.

121. Gordon Corera, *How Britain Pioneered Cable-Cutting in World War One,* BBC NEWS (Dec. 15, 2017), https://www.bbc.com/news/world-europe-42367551; *see also* David Kenyon, *The Zimmermann Telegram: the Telegram that Brought America into the First World War*, BBC: HISTORY EXTRA (Feb. 28, 2019, 3:40 PM), https://www.historyextra.com/period/first-world-war/zimmermann-telegram-brought-america-us-into-ww1-code-breaking-signit-germany-mexico (noting Britain cut and appropriated German telegraph cables after the war began, clandestinely reading messages.).

effect as used to be achieved in, say, World War II by bombing the London docks or taking out a power station by going after the physical infrastructure of cyberspace in the form of Internet undersea cables."[122] Others note that cutting undersea cables would be "the ultimate denial-of-service cyber weapon."[123] Yet, there has been no international movement to specially protect submarine cables during times of war.

Prominent legal experts warn that "the present legal regime is deficient in ensuring the security of cables."[124] Even those with more optimistic views of the "deficiencies of the existing legal regime," like Professor Wolff Heintschel von Heinegg of the NATO Cooperative Cyber Defense Centre of Excellence, admit that "the current legal regime has gaps and loopholes, and that it no longer adequately protects submarine cables," forcing states "to exert increased efforts" to provide sufficient protection.[125] The U.N. Convention on the Law of the Sea, which does not apply to wartime activities, merely recognized the right to lay international submarine cables,[126] as well as, obligating states to protect cables inside their territorial waters[127] and to domestically criminalize breaking or injuring cables.[128] Importantly, it does not protect cables beyond national jurisdiction.[129] Though states might lawfully be able to assert jurisdictional control and exercise defense of sovereign property under passive nationality or the protective principle during peacetime, or out of national self-defense during conflict, neither the Convention for the Protection of Undersea Telegraph Cables nor the United Nations Convention on the Law of the Sea, imposes a legal obligation on belligerents not to target the cables during wartime.[130] These shortcomings in the submarine cable protection regime show that this area is woefully in need of international protections, especially because a cut cable could

122. Barker, *supra* note 66.

123. Weintz, *supra* note 22.

124. Davenport, *supra* note 119, at 108; *see* also Robert Beckman, *Submarine Cablesa Critically Important but Neglected Area of the Law of the Sea*, *in* 7TH INTERNATIONAL CONFERENCE ON LEGAL REGIMES OF SEA, AIR, SPACE AND ANTARCTICA (2010).

125. Wolff Heintschel von Heinegg, *Protecting Critical Submarine Cyber Infrastructure: Legal Status and Protection of Submarine Communications Cables Under International Law, in* PEACETIME REGIME FOR STATE ACTIVITIES IN CYBERSPACE 291, 309-10 (Katharina Ziolkowsi ed., 2013).

126. U.N. Convention on the Law of the Sea, arts. 79, 112, Dec. 10, 1982, 1833 U.N.T.S. 397. (permitting all nations to place on continental shelf and high seas respectively). Note also art. 51(2), which permits maintenance of existing cables in archipelagic waters.

127. *Id.* at art. 21(1)(c).

128. *Id.* at arts. 113-15.

129. *See generally id.* at arts. 79, 113-15, 1833 U.N.T.S. at 430, 440.

130. von Heinegg, *supra* note 125, at 317.

impact civilians around the world, including those in states not party to the conflict.

IV. LEGALITY OF ACTIONS THAT TERMINATE CIVILIAN INTERNET CONNECTIVITY

Because LOAC applies as *lex specialis*, military actions would likely be judged under the traditional principles of necessity, distinction, proportionality, and humanity, as well as the rule that "attacks shall be limited strictly to military objectives."[131] This raises a preliminary question whether an action which cuts civilian internet access even constitutes an 'attack' under LOAC. In light of commentary and international holdings in this area, there is a substantial risk that military actions to shut off civilian internet connectivity might not constitute an 'attack,' which would provide the operative legal trigger for shifting from peacetime to the LOAC-governed armed conflict paradigm, and thus the limited protections afforded under LOAC might not apply at all. Furthermore, even if LOAC would apply, the deference given to military commanders, difficulties in quantifying harms and separating uses, and other deficiencies with traditional IHL principles render such protections insufficient to safeguard civilian internet connectivity.

A. Operations Against Civilian Internet Access Are Unlikely to Constitute 'Attacks' under LOAC

A "terminological gap [exists] between the legal and non-legal communities" regarding the meaning of the word "attack."[132] Computer network administrators often refer to an "attack" as "actions taken through the use of computer networks to disrupt, deny, degrade or destroy information."[133] This encompasses a broad range of actions, which cause no physical damage but could significantly disrupt civilian internet access. For example, a denial of service (DoS) operation preventing users from accessing a website would be considered in layman's terms an 'attack,' as would hackers entering a network to gather stored financial data. However, within the international legal community, the term 'attack' conveys legal meaning triggering rights and remedies, including the justification to respond with physical force.[134]

---

131. Additional Protocol I, *supra* note 90, at art. 52(1).

132. Michael N. Schmitt, *'Attack' as a Term of Art in International Law: The Cyber Operations Context*, *in* 2012 4TH INT'L CONFERENCE ON CYBER CONFLICT 283, 284 (Christian Czosseck et al. eds., 2012).

133. U.S. DEP'T OF DEFENSE, DOD DICTIONARY OF MILITARY AND ASSOCIATED TERMS 95 (2010) (defining "computer network attack").

134. *See* U.S. DEP'T OF DEFENSE OFFICE OF GEN. COUNSEL, LAW OF WAR MANUAL 47-48 (2015) (updated Dec. 2016) [hereinafter Law of War Manual].

1. It Is Unclear Whether Cutting Internet Access without Physical Destruction Would Be an "Armed Attack"

The presence of an 'attack' is important in determining whether the resort to force is lawful (*jus ad bellum*) and how conflicts may be fought (*jus in bello*). In *jus ad bellum,* an armed attack provides the right to respond with force under international law.[135] Under *jus in bello*, many provisions protecting civilians and civilian objects refer to an "attack."[136] The term operates equally in international and non-international armed conflict.[137] Because an "attack" constitutes an important operative threshold justifying "acts of violence" against an adversary, practitioners must assess whether actions constitute attacks.[138] One could argue that actions that sever civilian internet access are not legal "attacks" because they lack immediate violent harm to a human person. Yet textually, 'violence' is characterized by "intense . . . often destructive action or force,"[139] which is not confined to physical harm. Clearly, a widespread internet outage's destructive impacts could be costly and grave.

Since LOAC does not allow states to respond with force absent an "attack," courts and legal scholars have debated the meaning of this term. Some argue that the term "armed attack" in the U.N. Charter can be understood as "armed aggression," based on the equally authentic French translation "*aggression armee*."[140] The ICJ in *Nicaragua*, considered what constitutes an "armed attack," holding that while American training, arming, equipping, and supplying paramilitary forces conducting armed insurgency against the Nicaraguan government was wrongful, it did not constitute a threat or use of force ('armed attack') such that Nicaragua could lawfully resort

---

135. YORAM DINSTEIN, WAR, AGGRESSION AND SELF-DEFENSE 213 (5th ed. 2011) (referring to UN Charter Art. 51).

136. *E.g.*, Additional Protocol I, *supra* note 90, at art. 52(1).

137. *Treaties, States Parties and Commentaries: 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, Commentary of 1987,* INT'L COMM. OF THE RED CROSS, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Comment.xsp?action=openDocument&documentId=2C8494C2FCAF8B27C12563CD0043AA67 (last visited Jan. 14, 2021) ("Protocol I [, relating to International Armed Conflicts,] defines attacks. This term has the same meaning in Protocol II [, relating to Non-International Armed Conflicts]")..

138. Additional Protocol I, *supra* note 90, at arts. 48-49; *see also* MICHAEL N. SCHMITT ET AL., THE MANUAL ON THE LAW OF NON-INTERNATIONAL ARMED CONFLICT WITH COMMENTARY § 1.1.6 (2006) (drafters intended same meaning for 'attack').

139. Mix, *supra* note 11, at 90.

140. ÖYKÜ IRMAKKESEN, THE NOTION OF ARMED ATTACK UNDER THE UN CHARTER AND THE NOTION OF INTERNATIONAL ARMED CONFLICT – INTERRELATED OR DISTINCT? 4 (2014).

to armed countermeasures in self-defense.[141] The Court did not elaborate a precise test for when low-level actions might constitute an "armed attack," but said the "scale[,] effects," and "gravity" must be carefully considered.[142] Thus, according to the ICJ, the magnitude and nature of an 'attack' are directly related to whether physical force can be used in response. But the amount of 'force' necessary to cross the threshold remains disputed. States and jurists do not necessarily agree with the ICJ *Nicaragua* decision. Some set a high bar for the amount of force necessary to constitute 'armed attack', as is reflected in the U.N. General Assembly definition for aggression as something akin to a cross border military attack, invasion, bombardment, or blockade.[143]

The "legal definition of what exactly is a 'use of force' in the cyber realm is far less settled than in the kinetic realm."[144] Few states have articulated positions on what in the internet realm constitutes use of force commensurate with 'attack;' and when they do, their opinions lack definitive bright line parameters, offering only extreme examples.[145] Still these opinions help frame issues related to internet attacks, not just because cyber methods are often employed, but also because they illustrate the challenge of assessing true magnitude of digital harms. Harold Koh, a former U.S. State Department legal advisor, has proposed a test for whether a cyber action constitutes an attack or use of force; the test assesses "the context of the event, the actor perpetrating the action (recognizing challenging issues of attribution in cyberspace), the target and location, effects and intent, among other possible issues."[146] Koh's test seems difficult to satisfy because only "cyber activities that proximately result in death, injury,

---

141. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. Rep. 14 (June 27).

142. *Id.* at ¶¶ 195, 247, 249.

143. G.A. Res. 3314 (XXIX) at arts. 2-3 (Dec. 14, 1974).

144. Ryan Goodman, *Cyber Operation and the U.S. Definition of "Armed Attack*," JUST SEC. (Mar. 8, 2018), https://www.justsecurity.org/53495/cyber-operations-u-s-definition-armed-attack.

145. *See, e.g.*, Harold Hongju Koh, Legal Advisor, U.S. Dep't of State, Speech at U.S. Cyber Command Inter-Agency Legal Conference (Sept. 18, 2012) (transcript available at opiniojuris.org/2012/09/19/harold-koh-on-international-law-in-cyberspace/) (offering only extreme examples, "(1) operations that trigger a nuclear plant meltdown; (2) operations that open a dam above a populated area causing destruction; or (3) operations that disable air traffic control resulting in airplane crashes."); Brian J. Egan, Legal Advisor (former), U.S. Dep't of State, Speech at Berkeley Law: International Law and Stability in Cyberspace (Nov. 10, 2016), *in* 35 BERKELEY J. INT'L L. 169 (2017) (not offering specifics); Jeremy Wright, Attorney General (England and Wales), Speech at Chatham House: Cyber and International Law in the 21st Century (May 23, 2018) (transcript available at https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century).

146. Koh, *supra* note 145.

or significant destruction would likely be viewed as a use of force."[147] This would likely include blocking emergency communications, shutting down a prison internet system to release dangerous criminals into the public, crashing vehicles, and directly killing civilians by turning off internet-linked medical devices. The United Kingdom expresses similar views and has listed some extreme examples of cyberattacks that would qualify as attacks, e.g., triggering an urban nuclear meltdown or crashing a civilian jetliner.[148]

International jurists have created four main analytic models for assessing cyber attacks. These models are also applicable to actions against internet access that do not involve physical destruction.[149] The four models are the 'instrument-based' approach, 'effects-based' approach, 'actor-based' approach, and 'strict liability' approach. The 'instrument-based' approach considers whether the type of damage of caused by an internet action could previously have been caused by a kinetic attack. The 'effects-based' approach holistically looks to the severity of the consequences of the attack. Under the 'actor-based' approach, every action taken by the military would automatically constitute an armed attack regardless of the effects.[150] The 'strict liability' approach would consider any intrusion into a system an armed attack.[151] The most commonly referenced approach is the 'Schmitt Analysis,'[152] in which Professor Schmitt articulates six criteria for evaluating cyber effects to determine whether a digital action constitutes an armed attack.[153] The Schmitt Analysis considers (1) the severity of the damage caused by the attack, (2) whether the attack's effects are felt immediately, (3) whether the attack is "directly tied" to the resulting consequences or whether the attack depends "on numerous contributory factors to operate," (4) whether the "act causing the harm . . . crosses into the target state," (5) whether the attack's effects are "easy to ascertain," and (6) whether the attack is "illegitimate absent some specific exception such as self-defense."[154] These factors might also apply in assessing internet shutdowns. Also

147. *Id.*

148. Wright, *supra* note 145 ("[T]he UK considers it clear that cyber operations that result in, or present an imminent threat of, death and destruction on an equivalent scale to an armed attack will give rise to [a right to self-defense].").

149. Matthew J. Sklerov, *Chapter 4. Responding to International Cyber Attacks as Acts of War*, *in* INSIDE CYBER WARFARE: MAPPING THE CYBER UNDERWORLD 45 (Jeffery Carr ed., 2d ed., 2009).

150. *See e.g.* Paul A. Walker, *Rethinking Computer Network "Attack": Implications for Law and U.S. Doctrine*, 1 NAT'L SECURITY L. BRIEF 33, 34 (2011).

151. Sklerov, *supra* note 149.

152. Andrew C. Foltz, *Stuxnet, Schmitt Analysis, and the Cyber "Use-of-Force" Debate*, 67 JOINT FORCES Q. 40, 43 (2012).

153. Michael Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COL. J. TRANSNAT'L L. 885, 913–15 (1999).

154. *Id.*

relevant but lacking in detail is the Tallinn Manual, a study on international law and cyber warfare by a group of experts, which notes that most cyber activities generally would not constitute a 'use of force.'[155] Although these views are helpful, given the complete lack of international jurisprudence and scant recitations of state views, it is nearly impossible to conclusively determine what constitutes use of force under present international law. This is a "limbo period in which legal uncertainty and factual uncertainty remain at . . . high levels."[156]

Likewise, internet blackouts caused by 'flipping-the-switch,' unplugging communications cables, or using DoS to block access may not qualify as "attacks," particularly because these activities do not cause immediate physical destruction. Different tests might produce discrepant results. An actor-focused test might find any disruption of the internet to be an 'armed attack' if ordered by a military commander. An instrument-based test could find that a cut submarine cable constitutes physical damage and find that an 'armed attack' had occurred even if the consequence is merely an interruption or downgrading of digital communications. Conversely, under the 'effects test,' an electronic attack that erases all the financial, medical, criminal, and tax data in a country might not be considered an 'armed attack' because such a consequence would not be achieved with a conventional kinetic weapon (short of bombing all the servers and computers). "[E]ven though websites and content are unavailable for a period of time there is no [proximate] resulting physical damage or destruction of property" and thus the attack "would not be considered [to have] violent consequences," and therefore would not constitute an attack.[157] Referring to the Iranian government action which took the Saudi Aramco company's computer system offline and erased some of its data, legal observer Cassondra Mix concluded that the "destruction of data would be considered physical damage to property[, a] violent consequence," making the operation an 'attack.'[158] However, in the 2011 Egyptian 'flip-the-switch' internet blackout, Mix found that ordering the country's four internet Service Providers to block services for five days did not constitute an 'attack' because there were "no direct violent consequences," and the action "did not inflict death, bodily harm, damage, or destruction of property."[159] She argued that because financial harms are not generally considered property damage under LOAC and the physical harms are indirect or nonimmediate, "shutting down internet access is not

155. TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS, at art. 52 (Michael N. Schmitt ed., 2d ed. 2017) at art. 52.

156. Goodman, *supra* note 144.

157. Mix, *supra* note 11, at 94.

158. *Id.* at 95.

159. *Id.* at 98.

an attack."[160] Yet, Mix's specific conclusion is based on Egypt not being in an armed conflict at the time of the internet blockage, the relatively short in duration, and the lack of physical or lasting damage might not be extrapolated to more severe contexts. Moreover, it would be difficult to measure and assess attenuated and non-immediate harms, even if severe, under any test.

Put simply, the current legal system lacks a unified framework for determining whether an action against the internet constitutes an 'attack.' This uncertainty regarding what constitutes an 'attack' is problematic, because if there is no 'use of force,' then the LOAC may not apply for the purposes of taking defensive measures. This means there could be situations where civilian internet access has been severed, but states do not even have the basic right to take physical action in self-defense.

This uncertainty can be seen in practice. For example, the U.S. historically set a very low bar for the amount of force necessary to constitute an 'armed attack,' but simultaneously, sets a high bar for what should be considered an 'attack' in the cyber realm.[161] Doctrinally, the U.S. Department of Defense (DoD) Law of War Manual notes: "'cyber attacks' or 'computer network attacks' are not necessarily 'armed attacks' for the purposes of triggering a State's inherent right of self-defense under *jus ad bellum*."[162] This policy was seen in practice in February 2019 when, according to the Washington Post, U.S. Cyber Command conducted offensive cyber operations against Russian-government-linked hackers suspected of interfering with U.S elections.[163] Sources said the presidentially-approved mission "took the [Russian hackers] offline " likely using malware or a DoS attack.[164] Professor Paul Rosenzweig, observed that "if the U.S. had done so using a missile . . . it would have been an armed attack. . . . [Y]et somehow, in doing it via [internet] means, the [U.S.] has managed to avoid [the implication of an 'armed attack'], evaded public scrutiny . . . and possibly set a new standard for 'sub-warlike' cyber activity and beg[in] the creation of new international norms of behavior in the domain."[165] This example clearly illustrates the

160. *Id.* at 96.

161. Law of War Manual, *supra* note 134, at 1017 ("The United States has long taken the position that the inherent right of self-defense potentially applies against *any* illegal use of force.") (emphasis added).

162. *Id.* at 1013.

163. Ellen Nakashima, *U.S. Cyber Command Operation Disrupted Internet Access of Russian Troll Factory on Day of 2018 Midterms*, WASH. POST (Feb. 27, 2019), https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html.

164. *Id.*

165. Paul Rosenzweig, *The New Contours of Cyber Conflict*, LAWFARE (Feb. 27, 2019, 12:19 PM), https://www.lawfareblog.com/new-contours-cyber-conflict.

willingness of the U.S. to block an adversary's internet connectivity (albeit on a narrow basis), but also illustrates the difficulty in ascribing specific legal meaning to state practices relative to internet shutdowns. On one hand, the shutdown of the Russian hackers' internet systems could mean the U.S. believed the cyber intrusion and political interference constituted an imminent 'attack on American political independence,' warranting a proportionate defensive response. On the other hand, it could also indicate the U.S. did not find Russia's attack significant enough to constitute an 'armed attack' and thus responded in kind with something below the legal threshold of 'armed attack.' The incident illustrates the difficulty of defining 'armed attack' when dealing with internet shutdowns, especially when accomplished without physical destruction of communications infrastructure.

2. Actions Below the Threshold of 'Armed Attack' May Still be Improper Under International Law

There is almost no legal consensus with regard to what constitutes a wrongful cyber operation below the threshold of an 'armed attack.'[166] This is concerning because "all, or almost all of the conflict . . . in cyberspace occurs at the sub-'armed attack' level."[167] Yet activities below the threshold of an 'armed attack' could still be impermissible under international law. In *Nicaragua*, the ICJ recognized as wrongful activities that "do not constitute an armed attack but may nevertheless involve a use of force [prohibited by the U.N. Charter]."[168] To the Court, "the most grave forms of the use of force" needed to be distinguished from "other less grave forms,"[169] just as the U.N. Charter dictates that "other breaches of the peace" should be avoided.[170] Attacks on internet access using cyber techniques, such as DoS operations, targeted malware, and widespread domain name system confusion might fall below the threshold for 'armed attack' or serious 'use of force.' But in these instances, civilian populations might still be impacted by a clear 'breach of the peace.' It thus remains unclear what international rules, if any, would apply to protect civilian internet access from actions deemed to be 'less grave forms of use of force' falling below the threshold of 'armed attack,' as LOAC would not be

166. *Peacetime Cyber Espionage*, INT'L CYBER LAW IN PRACTICE: INTERACTIVE TOOLKIT, https://cyberlaw.ccdcoe.org/w/index.php?title=Peacetime_cyber_espionage&oldid=1930 (last visited Nov. 6, 2019).

167. Paul Rosenzweig, *Tallinn 2.0*, LAWFARE (Apr. 27, 2015, 12:57 PM), https://www.lawfareblog.com/tallinn-20.

168. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. Rep. 14, ¶ 210 (June 27).

169. *Id.* at ¶ 191.

170. U.N. Charter art. 1, ¶ 1.

triggered and IHRL would not govern outside of the perpetrators' areas of control.

B. Applying Traditional LOAC Principles to Shutdowns is Challenging and Does Not Adequately Protect Internet Connectivity

The traditional LOAC principles provide a framework for examining military actions during armed conflict. However, the framework is difficult to apply to civilian internet access disruptions for several reasons. First, the principle of necessity is difficult to apply to objects that provide general services to the public. Second, the principle of distinction is difficult to apply, because the internet may be used for civilian and military purposes, and it is challenging to distinguish between military and civilian communications. Third, the proportionality principle is difficult to apply, because it is difficult to measure the civilian harms that result from cyber attacks, and because military commanders are given significant deference when weighing these considerations. Lastly, the principles of avoiding unnecessary suffering and humanity do not provide sufficient protections, since they have traditionally only been applied to indispensable objects, which if deprived would result in physical starvation.

1. Necessity

Dr. Francis Lieber, a Columbia Law School professor asked by President Lincoln to articulate customary LOAC during the American Civil War, stated that only "measures which are indispensable for securing the ends of the war, and which are lawful according to the modern law and usages of war" are permitted.[171] With regards to civilian objects, Lieber said military necessity "allows of all destruction of property, and obstructions of the ways and channels of traffic, travel, or communication[.]"[172] In the modern era, the internet is clearly a channel of communication. To be lawful, terminating enemy internet connectivity must provide some sort of military advantage. Additional Protocol I says that "military objectives are limited to those objects which by their nature, location, purpose, or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization . . . offers a definite military advantage."[173] If the enemy utilizes the internet for command and control, or for military communications, the related military

171. FRANCIS LIEBER, WAR DEP'T, ADJUTANT GEN.'S OFFICE, INSTRUCTIONS FOR THE GOVERNMENT OF ARMIES OF THE UNITED STATES IN THE FIELD, GENERAL ORDERS NO. 100, at art. 14 (Apr. 24, 1863). [hereinafter Lieber Code].

172. *Id.* at art. 15.

173. Additional Protocol I, *supra* note 90, at art. 52(2).

advantage may be clear. However, when the link is more attenuated or connected to economic, public morale, or information warfare, attacks on internet infrastructure would be more suspect.

The International Committee of the Red Cross and the U.S. apply a "two-part" test to determine the necessity of attacks on objects such as infrastructure.[174] To be considered a legitimate military objective, the object must make "an effective contribution to military action" and "attacking [the] object, in the circumstances, [must] offer[] a definite military advantage."[175] These tests are hard to apply when traditionally civilian objects are targeted, as illustrated by the Eritrea-Ethiopia Claims Commission's difficulty determining whether military necessity justified an attack on a civilian power plant.[176] There, a majority of commissioners found that disabling a civilian power station could "qualify as a military objective during armed conflict" if it was of "sufficient importance to [an adversary's] capacity to meet its wartime needs of communication, transport and industry."[177] The Commission's majority emphasized that "economic importance" and "value [of producing power] to the country at war . . . [created] military significance" and may have "made an effective contribution to military action," such that it could lawfully be targeted as a military objective.[178] It found "the infliction of economic losses . . . a lawful means of achiev[ing] a definite military advantage."[179] However, Commission President Hans van Houtte strongly dissented, countering that civilian objects should not be targeted based on "hypothetical or speculative effects," which to him were "not sufficient," arguing that "the infliction of economic loss or the undermining of morale through the destruction of a civilian object . . . do not make that object a military objective."[180] He asserted that "an object is entitled to full protection" unless that object "makes an effective contribution to the enemy," and "its destruction, capture or neutralization provides a definite military advantage."[181] The fact that this esteemed panel could find a military leader's decision to target the civilian facility permitted by LOAC due to military 'necessity' suggests that specific and stronger protections are needed for civilian internet access, because commanders could

174. *See* INT'L COMM. OF THE RED CROSS, COMMENTARY ON THE ADDITIONAL PROTOCOLS TO THE GENEVA CONVENTION 635 (Yves Sandoz et al. eds.1978); Law of War Manual, *supra* note 134, at 208.

175. *Id.*

176. Western Front, Aerial Bombardment and Related Claims (Eri. v. Eth.), 26 R.I.A.A. 291, 334 (Eritrea-Ethiopia Cl. Comm'n 2005) [hereinafter Eritrea-Ethiopia Claims Commission].

177. *Id.*

178. *Id.*

179. *Id.* at 335.

180. *Id.* at 347 (separate opinion by President Hans van Houtte).

181. *Id.* at 346.

likewise argue that attacks on the civilian internet provide similar attenuated military advantages.

The U.S. Department of Defense has occasionally found that attacking civilian communications stations and economic assets was justified by military necessity. The U.S. used 'military necessity' to justify targeting Islamic State oil trucks because oil was the terrorist caliphate's primary economic engine, and destroying the trucks would hinder their ability to fight, providing a concrete military advantage.[182] Similarly, in 1999, U.S.-led NATO strikes attacked SerbTV, which the British and U.S. leadership described as an "entirely justified" attack on the "apparatus of dictatorship" because "the propaganda machine is prolonging the war. . . . [I]t's a legitimate target."[183] However, the attack drew heavy criticism and Judge George Aldrich, a U.S. negotiator of the peace agreement with North Vietnam and drafter of Additional Protocol I, contending that "[e]ven if . . . one were to conclude that certain television studios in Yugoslavia were, through their propaganda, making an effective contribution to military action, it would not necessarily follow that their destruction 'offers a definite military advantage,' as required by Article 52 of Protocol I."[184] In the digital realm, observers have noted that "[a] server hosting a social media site used by [violent insurrectionist] protestors for communication would be a military objective because it allows communication between protestors and its destruction offers a definite military advantage."[185] These examples illustrate the challenge in applying the principle of necessity to attacks on objects which provide general services to the entire population, including armed forces, and therefore necessarily make an effective contribution to military action.

2. Distinction

182. Aurel Sari, *Trucker's Hitch: Targeting ISIL Oil Transport Trucks and the Need for Advanced Warnings*, LAWFARE (Dec. 2, 2015, 2:12 PM), https://www.lawfareblog.com/truckers-hitch-targeting-isil-oil-transport-trucks-and-need-advanced-warnings.

183. Richard Norton-Taylor, *Serb TV Station was Legitimate Target, Says Blair*, THE GUARDIAN (Apr. 23, 1999, 10:20 PM), https://www.theguardian.com/world/1999/apr/24/balkans3#:~:text=Nato%20leaders%20yesterday%20scrambled%20to,of%20targets%20now%20considered%20legitimate (quoting Clare Short, International Development Secretary (UK)); Paul Richter, *Groups Protest Fatal Bombing of TV Facilities*, L.A. TIMES (Apr. 24, 1999, 12:00 AM), https://www.latimes.com/archives/la-xpm-1999-apr-24-mn-30651-story.html (quoting Kenneth Bacon:"[Serb TV] is as much a part of Milosevic's murder machine as his army.").

184. George H. Aldrich, *Yugoslavia's Television Studios as Military Objectives*, 1 INT'L L.F. DU DROIT INT'L 149, 150 (1999); *see also* Theodor Meron, *The Humanization of Humanitarian Law*, 94 AM. J. INT'L L. 239, 276 (2000) (agreeing that Aldrich's assessment of unlawfulness "seems accurate.").

185. Mix, *supra* note 11, at 89.

Under LOAC, belligerents have a duty to identify and differentiate between civilian and military objects, because through identification and separation civilians can be protected from violence of war.[186] This principle is of paramount importance when planning action against the enemy (referred to a 'targeting' in military circles). However, when it comes to internet access, distinguishing between military and civilian objects is difficult because both belligerents and civilians rely on the same internet connectivity and underlying physical infrastructure. With current technology, it is difficult to separate military digital communications from civilian use. Relatedly, LOAC prohibits 'indiscriminate attacks.'[187] However, as a practical matter, discriminating between military and civilian targets may not be feasible. While some highly advanced militaries might be able to selectively target and block the connectivity of selected users in limited circumstances, the reality is that militaries attempting to thwart enemy digital communications have no way of technically distinguishing between military and civilian communications. In this sense, military commanders' options when considering attacks on internet connectivity are currently all or nothing. This practical inability to distinguish fundamentally frustrates distinction analysis.

LOAC has long recognized that "attacks shall be limited strictly to military objectives."[188] Additional Protocol I dictates that, "to ensure respect for and protection of the civilian population and civilian objects, [belligerents] shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives . . . direct[ing] their operations *only against military objectives*" which "by their nature, location, purpose, or use make an effective contribution to military action and whose total or partial destruction, capture, or neutralization offers a definite military advantage."[189] "In case of doubt whether an object, which is normally dedicated to civilian purposes . . . is being used to make an effective contribution to military action, it shall be presumed not to be so used."[190] Internet connectivity must be viewed as 'dual use' because it benefits both combatants and civilians. As such, military commanders should presume civilian function for the internet, unless something indicates the adversary has taken full control of the internet from civilians.

---

186. The customary rule is codified in Additional Protocol I, *supra* note 90, at art. 48 ("In order to ensure respect for and the protection of the civilian population and civilian objects, the Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives.").

187. *Id.* at art. 51(4).

188. *Id.* at art. 52(1).

189. *Id.* at arts. 48 & 52 (emphasis added).

190. *Id.* at art. 52(3).

The LOAC principle of distinction also forbids indiscriminate actions. Additional Protocol I defines 'indiscriminate attacks' as those that either are not or cannot be directed at a specific military objective such that they "consequentially . . . are of a nature to strike military objectives and civilians or civilian objects without distinction."[191] Blanket actions that disconnect all civilian internet connectivity would appear to be indiscriminate, especially if means and methods are available to tailor the actions, such as focusing on specific regions, internet addresses, computer systems, or cell sites. An action that cuts a community's internet in a broad attack that causes economic damages, societal harm, and circumscribes civilians' fundamental right to communicate, without distinguishing between civilians and combatants would frustrate the principle which requires refraining from indiscriminate actions. Assuming more tailored options exist, the resulting civilian harm could be considered 'unnecessary suffering,' which is unlawful under LOAC. Because actions against the internet must be focused, rather than indiscriminate, operations shutting down internet access to an entire population create the appearance of indiscriminate action forbidden by LOAC.

3. Proportionality

Under LOAC, military commanders must weigh the military advantage gained from an attack against the expected incidental harm to civilians and civilian objects.[192] Proportionality has been codified in Article 57 of Protocol I, which says states parties must "refrain from deciding to launch any attack which may be expected to cause . . . damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated."[193] It requires that "those who plan or decide upon an act shall . . . take all feasible precautions in the choice of means and methods of attack with a view to avoiding [or] minimizing . . . damage to civilian objects."[194] Despite the requirements, there are no set standards for weighing the extent of civilian harm, and no means to verify that all feasible precautions have been taken. Military commanders are free to use their best judgement (often with the help of Judge Advocates, legal advisors, and collateral damage experts). In the context actions which severe civilian internet access, it is difficult

191. *Id.*

192. *See* Schmitt, *supra* note 138, at 293.

193. Additional Protocol I, *supra* note 90, at art. 57(2)(a)(iii).

194. *Id.* The treaty does not define 'feasible precautions,' but many states have held it to mean "precautions which are practicable or practically possible taking into account all circumstances ruling at the time, including humanitarian and military considerations." *Customary IHL Database-Practice Relating to Rule 15. The Principle of Precautions in Attack*, INT'L COMM. OF THE RED CROSS: IHL DATABASE, https://ihl-databases.icrc.org/customary-ihl/eng/docs/v2_rul_rule15_sectionc (accessed on Nov 21, 2020).

to apply traditional proportionality analysis because of the challenge of weighing the harms these operations cause. This challenge of measuring civilian harm combined with unfettered discretion and leeway could result in legal ambiguity without reliable and functional safeguards for civilian internet connectivity during armed conflict.

a. It Is Nearly Impossible to Assess the Extent of Civilian Harm

Balancing the value of the expected military advantage against the civilian harm is inherently challenging. Under proportionality analysis, significant incidental harms to civilians would be tolerated to achieve an extremely important military objective. In the ICJ's split decision on the use of nuclear weapons, seven judges found the use of nuclear weapons might be permitted "in an extreme circumstance or self-defense, in which the very survival of the State would be at stake," whereas the dissent felt that "it cannot be accepted that the use of nuclear weapons on a scale which would – or could – result in the deaths of many millions in indiscriminate inferno . . . could be lawful."[195] This split decision reflects the great challenge of conducting a proportionality analysis when the magnitude of harm is great, and where the effects are indiscriminate and widespread. Similarly, assessing whether a civilian internet shutdown is proportionate would be challenging because civilian harms are distributed and temporally delayed. Observers find that even activities which "affect the entire population of a state," such as destabilizing financial systems or tampering with an electoral system, may be "too diffuse and low-level" for international law to apply.[196]

Additional Protocol I says that "civilians shall enjoy general protection against dangers arising from military operations" but this provision only applies to in the context of "attacks" involving "acts or threats of violence," which suggests limited to situations where civilians might suffer physical injury (or severe mental suffering) or tangible property damage.[197] Experts suggest that, for the purposes of determining proportionality, only "loss of civilian life, injury to civilians [and] damage to civilian objects" should be considered, while "mere inconvenience would not suffice."[198] Under Professor Deeks'

195. Legality of the Threat or Use of Nuclear Weapons, *supra* note 83, at 311 (Schwebel, V.P., dissenting).

196. Ashley S. Deeks, *Confronting and Adapting: Intelligence Agencies and International Law*, 102 VA. L. REV. 599, 672 (2016).

197. *See* Additional Protocol I, *supra note* 90, at arts. 51(1)-(2). ("civilians shall enjoy general protection against dangers arising from military operations [including] acts or threats of violence."). *See also*, Ido Kilovaty, *Virtual Violence - Disruptive Cyberspace Operations as "Attacks" Under International Humanitarian Law*, 23 MICH. TELECOMM. & TECH. L. REV. 113, 117,127 (2016).

198. Michael N. Schmitt, *War, Technology and the Law of Armed Conflict*, 82 INT'L L. STUD. 137, 156 (2006) (emphasis omitted).

pragmatic, if legally dissatisfying approach, "the more serious and direct the [resultant] harm . . . the less leeway a state should have in interpreting provisions of potentially applicable treaties or [customary international law]."[199] Commanders assessing the magnitude of civilian harm that may result from cutting or restricting internet connectivity will be challenged to separate and quantify the reasonably foreseeable effects, which must be considered, from merely speculative harms. Without clear guidelines, military commanders might be more inclined to cut off civilian internet access without fully appreciating the magnitude of civilian harm.

b. It Is Similarly Difficult to Assess Which Civilian-Protecting Precautions Are Required

The proportionality principle also requires belligerents to take careful precautions to protect civilians. Any attack where feasible precautions are not taken is excessive and unlawful.[200] Additional Protocol I requires that states "do everything feasible to verify that objectives to be attacked are neither civilians or civilian objects." It also requires commanders to "take all feasible precautions in choice of means and methods [to avoid or minimize] injury to civilians and damage to civilian objects," and "to refrain if [the impact on civilians] would be excessive in relation to the concrete and direct military advantage anticipated."[201] The International Criminal Tribunal for the Former Yugoslavia found that customary international law also imposed this duty to take precautions.[202] Still, reasonable minds may disagree about which precautions are feasible.

This requirement creates heightened obligations for technically sophisticated belligerents. This additional factor makes the proportionality analysis even more amorphous. Technically advanced powers can launch more targeted operations and therefore can minimize harm to civilians. Such states have robust intelligence platforms, as well as technological cyber capabilities, to better focus operations specifically against enemy connectivity rather than imposing widespread cuts to civilian internet access. These powers must take all feasible steps to fulfill their obligation to mitigate collateral damage and incidental harms. In this way, the higher a belligerent's technical competence and the greater its responsibility to exercise greater precision, the less likely that a complete blackout of an adversary's civilian internet would be lawful. Less advanced

199. Deeks, *supra* note 196, at 672.

200. Additional Protocol I, *supra* note 90, at art. 57(2)(a); *see also*, Jean-Francois Queguiner, *Precautions Under the Law Governing the Conduct of Hostilities*, 88 INT'L REV. OF THE RED CROSS 793, 817 (2006).

201. Additional Protocol I, *supra* note 90, at art. 57(2)(a).

202. *See* Prosecutor v. Kupreškić et al., Case No. IT-95-16-T, Judgement, ¶ 524 (Int'l Crim. Trib. for the Former Yugoslavia Jan 14, 2000).

groups, whether they be non-state actors, resistance movements, or developing powers, should also be cognizant that while an attack on civilian internet of the more technically savvy opponent will give them an advantage, it may not substantially change the way that power fights, such that the military advantage gained would not outweigh the harm to civilians. However, in practice, without a clear analytic rubric for assessing civilian harms, even the most technically savvy belligerent will be confounded by proportionality analysis given the unknown harms and second or third-order effects.[203]

4. Humanity and Avoiding Unnecessary Suffering: Digital Starvation?

The LOAC has increasingly recognized the need to protect objects that are indispensable to the civilian population. While the 1863 Lieber Code found it "lawful to starve the hostile belligerent, armed or unarmed, [for] speedier subjugation of the enemy," the law has since changed.[204] After World War I in 1919, the Report of the Commission on Responsibility, an international body created by the Paris Peace Conference, observed that "'deliberate starvation of civilians' violates customary law of war."[205] Later, the 1949 Fourth Geneva Convention observed that belligerents "shall allow free passage of all consignments [or goods] of medical and hospital stores," "objects necessary for religious worship," and "essential foodstuffs, clothing, and tonics" for children under fifteen and expectant mothers, so long as these goods were not diverted to or otherwise help the enemy war effort.[206]

Additional Protocol I more explicitly protects objects necessary to the survival of the civilian population, stating that "starvation of civilians as a method of warfare is prohibited."[207] As Additional Protocol I states, "[i]t is prohibited to attack, destroy, remove or render useless *objects indispensable to the survival of the civilian population*."[208] Further, "it is prohibited to attack, destroy, remove or render useless objects indispensable to the survival of the civilian population, such as food-stuffs, agricultural areas, . . . crops, drinking water installations and supplies and irrigation works, for the specific

---

203. *See* LAURIE BLANK & GREGORY NOONE, INTERNATIONAL LAW AND ARMED CONFLICT: FUNDAMENTAL PRINCIPLES AND CONTEMPORARY CHALLENGES IN THE LAW OF WAR 534 (2d ed. 2018).

204. *See* Lieber Code, *supra* note 171 at art. 17.

205. *See* PARIS PEACE CONFERENCE, VIOLATIONS OF THE LAWS AND CUSTOMS OF WAR: REPORTS OF MAJORITY AND DISSENTING REPORTS AMERICAN AND JAPANESE MEMBERS OF THE COMMISSION OF RESPONSIBILITIES, CONFERENCE OF PARIS, 1919 at 33-34 (1919).

206. Fourth Geneva Convention, *supra* note 106, at art. 23.

207. Additional Protocol I, *supra* note 90, at art. 54.

208. *Id.* (emphasis added)

purpose of denying them for their sustenance value to the civilian population or to the adverse Party, whatever the motive, whether in order to starve out civilians, to cause them to move away, or for any other motive."[209] It provides only two exceptions for attacking or rendering useless indispensable civilian objects. First, a military may attack "sustenance solely for the members of [adversary's] armed forces."[210] Second, "if not sustenance," then a military may attack "in direct support of [adversary's] military action, provided . . . in no event shall actions against these objects be taken which may be expected to leave the civilian population with such inadequate food or water as to cause its starvation or force its movement."[211]

The anti-starving provisions of Additional Protocol I are binding on the 174 states that ratified it. However, these provisions also likely apply to all states as a matter of customary international law or *jus cogens*.[212] In 2005, the Eritrea-Ethiopia Claims Commission "conclude[ed] that the provisions of Article 54 that prohibit attack against drinking water installations and supplies that are indispensable to the survival of the civilian population for the specific purpose of denying them for their sustenance value . . . ha[ve] become part of customary international law."[213] The Commission observed trends towards customary status, noting that "none of the [over 160 states party] made any reservation or statement rejecting or limiting the binding nature of that prohibition" against attacking indispensable civilian objects regardless of the motive.[214] The Commission also observed that even nonparties, like the United States, accept as "customary rule" the prohibition on "intentional destruction of objects indispensable to the survival of the civilian population *for the specific purpose* of denying [civilian use]."[215]

However, if the Commission's interpretation of customary international law is correct, it would illustrate a fundamental weakness in the anti-starvation provisions: they only prohibit actions if the *mens rea* or "specific purpose" is harming the civilian population. So long

---

209. *Id.*

210. *Id.*

211. *Id.*

212. INT'L COMM. OF THE RED CROSS, *supra* note 95 (listing states-parties). Non-parties include the United States, Israel, Iran, Pakistan, India, and Turkey. *See, e.g.,* Michael J. Matheson, *Session One: The United States Position on the Relation of Customary International Law to the 1977 Protocols Additional to the 1949 Geneva Conventions, in* The Sixth Annual American Red Cross-Washington College of Law Conference on International Humanitarian Law: A Workshop on Customary International Law and the 1977 Protocols Additional to the 1949 Geneva Conventions, 2 AM. U.J. INT'L L. & POL'Y 419, 426 (1987) (State Department Legal Advisor: "[the U.S.] support[s] the principle that starvation of civilians not be used as a method of warfare.").

213. Eritrea-Ethiopia Claims Commission, *supra* note 176, at ¶ 105.

214. *Id.* at ¶ 104.

215. *Id.* (emphasis added).

as the belligerent had some other purpose, the intentional destruction of an indispensable civilian object might be permitted. This logic would permit cutting vital civilian internet access, as long as harming civilians was not the exclusive purpose of the action. However, the International Committee of the Red Cross questions this logic and instead suggests that a more accurate restatement of customary international law would recognize a broader prohibition against all actions against indispensable civilian objects, even when there are compelling military rationales for the action.[216]

One could argue that the internet constitutes 'sustenance' as it 'nourishes' the mind: people rely on the internet for socio-familial bonds, and entire populations depend on it for supporting logistical coordination. However, this would be a stretch legally. Traditional definitions of sustenance are limited to "food and drink."[217] Consequentially, under Additional Protocol I, if the internet were an 'indispensable' civilian object, action could only be lawfully taken against it if it directly supported adverse military action. But even then, an attack on the internet would not be lawful if it would leave the civilian population without necessities like food or water, or force civilian movement. Today, the internet helps ensure that the civilian population has access to necessities, like water and food. Production and distribution of crops, food supplies, remittances, and medicines are logistically managed over the internet. A case can surely be made that in modern society internet access might be indispensable under the LOAC.

However, the constrained the anti-starvation provisions expressed in Additional Protocol I render the expansion of such protections uncertain beyond their traditional application to 'water and foodstuffs.' Because of the disagreements over whether internet connectivity is truly 'indispensable' to the population, and the dispute over whether civilian populations can be starved if civilian harm is not the sole purpose of the action, existing LOAC provisions against starvation are inadequate to safeguard internet access.

V. APPLICABILITY OF SPECIAL PROTECTION REGIMES IN ARMED CONFLICT

Given the difficulties and ambiguities in applying traditional LOAC analysis to the uniqueness of the internet, one might instead look to specialized humanitarian protection regimes as a basis for protecting civilian internet access. LOAC has long recognized special

---

216. *See* HENCKAERTS & DOSWALD-BECK, *supra* note 112, at 189-193 (part of an official ICRC study asserting to restate customary international law, specifically under "Rule 54. Attacking, destroying, removing or rendering useless objects indispensable to the survival of the civilian population are prohibited.").

217. Additional Protocol I, *supra* note 90, at art. 54.

protections for specific persons and objects, such as the injured, humanitarian workers, and cultural treasures. This section analyzes these regimes and finds that while they do not adequately apply to nor protect civilian internet access, such specialized protection regimes could serve as models for protecting highly valued people and things during armed conflict. As such, a specialized protection regime would be a uniquely effective way to provide heightened protections for internet access under LOAC.

A. Emblematic Humanitarian Protections

Civilian hospitals not used for any unlawful military purpose "may in no circumstances be the object of attack, but shall at all times be respected and protected by parties to the conflict."[218] LOAC has adopted emblems such as the Red Cross and Red Crescent to denote special protection for medical and humanitarian aid personnel and facilities in conflict zones. Employment of these emblems is intended to identify and protect medical and relief workers, as well as military and civilian medical facilities during armed conflict.[219] The Geneva Conventions requires that "[p]arties to the conflict. . . take the necessary steps, in so far as military considerations permit, to make the distinctive emblems indicating medical units and establishments clearly visible to the enemy land, air or naval forces, in order to obviate the possibility of any hostile action."[220] Medical aircraft likewise "shall not be attacked" and "shall be respected while flying at heights, times and on routes specifically agreed upon between all the parties to the conflict."[221] With respect to protecting hospital ships, parties must "use the most modern methods available to facilitate the identification of [such ships]."[222] The ICRC succinctly describes the emblems' meaning as 'Don't Shoot!'[223]

Adopted during the original Geneva Conference in 1864, the red cross emblem was meant as an inversion of the Swiss flag (a white cross on red background) to represent neutrality in the conflict to protect those caring for the sick and wounded.[224] The committee had sought "a single emblem to protect ambulances and hospitals . . . that would be recognizable at a distance, universally accepted and backed

---

218. Fourth Geneva Convention, *supra* note 106, at art.18.

219. *See* First Geneva Convention, *supra* note 106, at arts. 39-44.; *see also Summary of the Geneva Conventions of 1949 and Their Additional Protocols*, AM. RED CROSS: INT'L HUMANITARIAN L. Apr.2011.

220. First Geneva Convention, *supra* note 106, at art. 42; Second Geneva Convention, *supra* note 106, at arts. 41-44.

221. Fourth Geneva Convention, *supra* note 106, at art. 22.

222. Second Geneva Convention, *supra* note 106, at art. 43.

223. *The Emblem*, BRITISH RED CROSS, https://www.redcross.org.uk/about-us/what-we-do/protecting-people-in-armed-conflict/the-emblem (last visited Apr. 5, 2020).

224. *See id.*

by law."[225] Later in 1877, the ICRC recognized the red crescent since the Ottomans felt the cross conveyed Christian symbology.[226] The Jewish red star of David used by the Israeli relief society has not been recognized by the ICRC or other body, but still warrants customary protection for relief workers.[227] Additional Protocol I prohibits misuse of "the distinctive emblem of the Red Cross, Red Crescent, or . . . other emblems, signs or signals [recognized under International Humanitarian Law]."[228] In 2005, a Third Additional Protocol was adopted providing for a new alternative emblem—the red crystal—that could be used in environments where another emblem might be misperceived as having religious, cultural or political connotations.[229] Additional Protocol I also adds additional protected symbols for civil defense forces and installations containing dangerous forces.[230] The Geneva Conventions criminalize misuse or other unauthorized employment of the emblems as a war crime.[231] The "perfidious use of the red cross or other emblem" specifically "shall be regarded as [a] grave breach[] of [Additional Protocol I]."[232] However, in view of the dangers hospitals face if located near to military objectives, "it is recommended that such hospitals be situated as far as possible from military objectives."[233] Recognizing the vital importance of medicine and aid, LOAC evolved to create a specialized regime based on emblems and markings.

Closely related, protections of medical personnel have been affirmed by international jurisprudence. In 1993, the U.N. Commission on the Truth for El Salvador found that the summary execution of a Spanish doctor who had gone to provide medical aid

---

225. Jonathan Benthall, *The Red Cross and Red Crescent Movement and Islamic Societies*, 24 BRIT. J. MIDDLE EASTERN STUD. 157, 159 (1997).

226. *See id.* at 160.

227. *See id.* at 163.

228. Additional Protocol I, *supra* note 90, at arts. 38, 85.

229. *See* Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Adoption of an Additional Distinctive Emblem (Protocol III), art. 2, 8 Dec. 2005, 2404 U.N.T.S. 261; *see also, Treaties, States Parties and Commentaries*: *Commentary on Protocol additional to the Geneva Conventions of 12 August 1949, and relating to the Adoption of an Additional Distinctive Emblem (Protocol III), 8 December 2005,,* INT'L COMM. OF THE RED CROSShttps://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Treaty.xsp?action=openDocument&documentId=8BC1504B556D2F80C125710F002F4B28 (last visited Jan. 13, 2021).

230. Additional Protocol I, *supra* note 90, at arts 16-17.

231. *See* First Geneva Convention, *supra* note 106, at art. 53 (assigning state responsibilities); *id.* at art. 54 (requiring parties enact domestic legislation to prevent and punish abuses of the emblems); Second Geneva Convention, *supra* note 106, at arts. 44-45.; Additional Protocol I, supra note 90, at art. 38 ("[I]t is prohibited to make improper use of the distinctive emblem . . . .").

232. Additional Protocol I, *supra* note 90, at art. 85.

233. Fourth Geneva Convention, *supra* note 106, at art. 18.

to a liberation movement violated international humanitarian law.[234] In Rwanda, the U.N. Commission of Experts reported that attacks on medical personnel were grave violations of international humanitarian law in 1994.[235] The 1995 U.N. Verification Mission in Guatemala found revolutionaries should refrain from "endangering ambulances and duly identified health workers who assist wounded persons."[236] In 2004, the U.N. Commission on Human Rights "strongly condemn[ed] the Israeli army [for] . . . opening fire on ambulances and paramedical personnel[, and] . . . preventing ambulances and vehicles of the [ICRC] from reaching the wounded and the dead in order to transport them to hospital, thus leaving the wounded bleeding to death in the streets."[237] Similarly, in 2006, the U.N. Human Rights Council condemned "the Israeli killing of Palestinian . . . medics in Beit Hanoun."[238]

B. Special Protections for Cultural Property

Throughout the evolution of LOAC, cultural and charitable property has received special protection both, as a matter of custom and also through multiple international treaties. The Lieber Code of 1863 required that "classical works of art, libraries, scientific collections, or precious instruments, such as astronomical telescopes . . . must be secured against all avoidable injury, even when they are contained in fortified places whilst besieged or bombarded."[239] This provision reflects the sentiment that precious cultural, scientific, and intellectual objects warrant special safeguarding because of their uniquely important role to the civilization. The 1907 draft of the treaty respecting the Laws and Customs of War on Land echoed the notion, stating that "all necessary steps must be taken to spare . . . buildings dedicated to religion, art, science, or charitable purposes and historical monuments," with the caveat that such buildings are not

234. *See* Rep. of the Comm'n on the Truth for El Salvador (1993), transmitted by Letter Dated 29 March 1993 from the Secretary-General Addressed to the President of the Security Council, at 89-92, U.N. Doc S/25500 (Apr. 1, 1993).

235. *See Final Rep. of U.N. Comm. of Experts Established Pursuant to Security Council Resolution 935* (1994), transmitted by Letter Dated 9 December 1994 from the Secretary-General Addressed to the President of the Security Council ¶¶ 73-92, 120, U.N. Doc. S/1994/1405 (Dec. 9, 1994).

236. Rep. of the Director of the U.N. Mission for the Verification of Human Rights and of Compliance with the Commitments of the Comprehensive Agreement on Human Rights in Guatemala, ¶ 194, U.N. Doc. A/49/856 (Mar. 1, 1995).

237. U.N. Comm'n on Human Rights Res. 2004/10, at ¶ 10 (Apr. 15, 2004).

238. Human Rights Council Res. S-3/L.1, U.N. Doc. A/HRC/S-3/L.1 (Nov. 14, 2006).

239. Lieber Code, *supra* note 171, art. 35.

being used for military purposes and the places be specially marked with "distinctive and visible signs."[240]

The Annex to the Hague IV Convention noted "all seizure of, destruction or willful damage done to . . . monuments, works of art and science, is forbidden, and should be made the subject of legal proceedings."[241] In 1954, the Convention for the Protection of Cultural Property in the Event of Armed Conflict went further, obliging states parties to "prohibit, prevent and, if necessary, put a stop to any form of theft, pillage or misappropriation of, and any acts of vandalism directed against, cultural property," defining cultural property broadly to include numerous objects, such as "monuments of architecture, art or history ... archaeological sites...works of art; manuscripts, books ... as well as scientific collections and important collections of books... ...museums, large libraries and depositories of archives."[242] The Convention has widespread adherence, with 133 states parties.[243] However, this Convention allows states parties to waive their obligation if "military necessity imperatively requires" damaging or destroying cultural property.[244] Yet the Convention provides even greater levels of protection for "cultural property of very great importance:" states parties must refrain "from any act of hostility" against this property, so long as the property is not used for any military purpose. But even then, the parties are required to "first request the cessation of such a violation," and notify a U.N. cultural body "in writing, stating the reasons" justifying action against the cultural property of great importance.[245]

A second protocol, signed in 1999, further enhances protection for cultural property; under this protocol, such property can only be targeted when "made into a military objective," and "no feasible alternative" offers a similar military advantage. Furthermore, even greater protection is warranted if "it is cultural heritage of the greatest importance for humanity" and is recognized for "exceptional cultural

240. Convention Respecting the Laws and Customs of War on Land, Annex: Regulations Concerning the Laws and Customs of War on Land, Annex at art. 27, Oct. 18, 1907, 36 Stat. 2277.

241. *Id.* at art. 56.

242. Convention for the Protection of Cultural Property in the Event of Armed Conflict, arts. 1 & 4, May 14, 1954, T.I.A.S. No. 09-313.1, 249 U.N.T.S. 215.

243. *See Treaties, States Parties and Commentaries: Convention for the Protection of Cultural Property in the Event of Armed Conflict. The Hague, 14 May 1954,* INT'L COMM. OF THE RED CROSS, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/States.xsp?xp_viewStates=XPages_NORMStatesParties&xp_treatySelected=400 (last visited Jan. 13, 2021).

244. Convention for the Protection of Cultural Property in the Event of Armed Conflict, *supra* note 242, at art 4.2.

245. *Id.* at arts. 8-11.

and historic value [to ensure] the highest level of protection."[246] For cultural property with the greatest importance for humanity as designated by the International Committee of the Blue Shield, this protocol requires high-level decision making and precautions to minimize damage if attacked.[247] Similarly, Additional Protocol I states, "it is prohibited . . . to commit any acts of hostility directed against historic monuments, works of art or places of worship which constitute the cultural or spiritual heritage of peoples."[248] This provides much greater protection than regular LOAC analysis.

Could civilian internet access be considered cultural property, and attain protected status under the existing special regime? The internet has certainly taken on a vital role in modern culture—serving as a repository of knowledge and avenue for maintaining cultural connections across great distances. Especially during conflict, the internet may provide people's only connection to cultural treasures, such as art, music, literature, and historical accounts. Thus, it could be argued that the internet constitutes protected 'cultural property' as a scientific wonder or for the culture it brings to civilians.

However, the nature of internet connectivity does not squarely fit into the cultural property paradigm, because it is not a discrete singular object which could be damaged or destroyed, but rather a means of accessing culture. Cultural property, under the Convention, consists of specific objects.[249] While a creative argument could be made that internet connectivity constitutes cultural property at every location where it is accessed, this would become unwieldly given the requirement that specific site lists be generated and validated. Still, the fact that the law recognizes the importance of cultural items during conflict underscores why internet access deserves similar protection. Many living in conflict zones would feel that a person's ability to communicate lifesaving humanitarian information to the present generation is as important as saving cultural artifacts for the future.

---

246. Second Protocol to the Hague Convention of 1954 for the Protection of Cultural Property in the Event of Armed Conflict, arts. 6 & 10, Mar. 26, 1999, 2253 U.N.T.S. 172.

247. *Id.* at arts. 11 & 13(applicable to cultural property of "greatest" importance as described in art. 10).

248. Additional Protocol I, *supra* note 90, at art. 53.

249. Convention for the Protection of Cultural Property in the event of Armed Conflict, *supra* note 242, at art. 1 (defining cultural property as "movable or immovable property of great importance to the cultural heritage of every people, such as monuments of architecture, art or history, whether religious or secular; archaeological sites; [buildings]... of historical or artistic interest; works of art; manuscripts, books and other objects of artistic, historical or archaeological interest; as well as scientific collections and important collections of books... [and] buildings whose main and effective purpose is to preserve or exhibit the movable cultural property... [e.g.] museums, large libraries and depositories of archives").

Rather than trying to imperfectly apply these cultural protections to internet connectivity, a new paradigm should be created to protect internet access. It can build on the lessons from the cultural property regime—such as the requirement for written determinations and highest-level decision-making—before widespread civilian internet connectivity can be terminated in war. This would allow for the internet, which may be among the most important objects for the practice and preservation of culture, to receive commensurate protection during conflict via a specialized protection regime.

VI. TOWARDS GREATER PROTECTION FOR CIVILIAN INTERNET CONNECTIVITY

In modern society, internet connectivity now plays a fundamental and unique role for individuals and populations as a whole, warranting recognition and special protections during armed conflict. This section proposes a number of options for ensuring greater legal protection for civilian internet access. These include both legal and technical proposals. First, countries could engage in global consensus-building and collaboration to articulate the new reality and develop new norms which recognize the humanitarian importance of internet connectivity. The failure to do so proactively may result in the practices of bad actors being tolerated by the global community, thereby establishing norms under customary international law that would permit depriving civilians of internet access during conflict. Indeed, this appears to already be occurring in non-international armed conflicts, where governments routinely cut off civilian internet access. Second, policymakers should start by specially protecting physical internet infrastructure, using the previously-discussed special protection regimes as a guide. Finally, states could employ digital emblems, and adopt technological changes in the form of special humanitarian VPNs and internet protocols to ensure that vital civilian communications can continue during armed conflict. Such protocols would digitally designate humanitarian networks and enable belligerents to distinguish between civilian and military targets, yielding greater protections under LOAC.

A. Recognizing A New Reality and New Norms

Lawrence Friedman noted that rules of law established by policymakers or enunciated by courts "lay down a stable and clear-cut principle by which men can govern their conduct." But if the rule doesn't comport with changing technologies, then there must be changes or exceptions to conform to "social fairness."[250] Similarly,

250. Andras Sajo & Clare Ryan, *Judicial Reasoning and New Technologies*, *in* THE INTERNET AND CONSTITUTIONAL LAW 3, 6 (Oreste Pollicino & Graziella

U.S. Supreme Court Justice Brandeis' now famous dissent in *Olmstead* notes that legal provisions guaranteeing "individual protection against specific abuses of power, must have a similar capacity of adaptation to a changing world."[251] The internet plays a vital role in modern society. This fact is currently reflected in IHRL, but not yet in LOAC. As this Article has discussed, traditional LOAC analysis offers some protection to internet infrastructure and requires consideration of civilian impacts during 'proportionality' analysis, but such basic and general protections inadequately safeguard civilian internet access during armed conflict. Instead, the global community should establish new protective norms.

This process would start by accepting some fundamental humanitarian truths: internet connectivity is necessary to coordinate civilian humanitarian logistics—including food and basic supplies, pharmaceutical management, medical records keeping, personal records, educational content, and the transmission of important news regarding public health risks. The global community should demand from the outset that any deprivation of internet connectivity be considered impermissible unless viable alternatives are offered. Finally, the global community should develop a uniform system of digital emblems to allow digital messages vital to the needs of the population to be exchanged in ways that do not prejudice parties to the conflict. The ICRC should take the lead, calling together experts and issuing interpretive guidance. The U.N. General Assembly should call on the International Law Commission to make recommendations for increasing internet access protections in international law. States should also endeavor to discuss the legality of attacks on the internet with their military commanders and legal advisors. Militaries should craft special Rules of Engagement, which raise decision making for civilian internet blackouts to high levels, and require written findings. Military lawyers should draft checklists and decision matrices to help commanders to weigh the full extent of potential civilian harm in proportionality analysis. These efforts will help to create global norms that give special recognition to internet connectivity.

B. Heightening Internet Infrastructure Protection During Wartime

While global internet infrastructure is vitally important to maintaining connectivity, it lacks adequate protection during armed conflict. Given its physical vulnerability—which poses a risk of

---

Romeo eds., 2016) (quoting Lawrence M. Friedman & Jack Ladinsky, Social Change and the Law of Industrial Accidents, 67 COLUM. L. REV. 50, 59 (1967)).

251. Olmstead v. United States, 277 U.S. 438, 472 (1928) (Brandeis, J., dissenting).

collateral damage to billions of people that rely on communications for their livelihoods—a framework should be enacted globally to protect physical internet communications systems. This framework should focus on adopting special protections for internet communications cables and the international community should consider a special emblem to protect physical internet infrastructure.

1. Special Protections for Internet Communications Cables

One step for heightening internet infrastructure protection during wartime is to adopt special protections for deep-sea submarine cables. This is particularly important, as these cables have no special wartime protection today. Any manipulation or physical destruction of such cables should be subject to international law as a wrongful act, even if it falls below the threshold of armed attack. While these cables certainly carry military communications, they also carry vital information necessary for billions of civilian enterprises, from trade to science, medicine, and humanitarian relief. Because current telecommunications law provides no specific protections applicable during wartime, only the traditional rules of armed conflict would constrain operations aimed at internet communications infrastructure. For example, a military commander or national authority could lawfully order the cutting off of internet access to an entire civilian population, if deemed 'necessary and proportionate.' While cutting enemy communications would undoubtedly provide a military advantage, the potential damage to the civilian population of cutting them off from the internet would be especially devastating during times of war. The global community could try, as was attempted with nuclear weapons and landmines, to develop a universal treaty prohibiting destruction of cables during war time, perhaps as an additional protocol to the Geneva Conventions. Some states will doubtless object and reserve the right to cut cables in times of extreme necessity. Nevertheless, the global community should expressly condemn the practice, so that no state takes the decision of shutting down civilian internet access lightly. Perhaps over time, if states avoided such actions during armed conflict, this practice would be considered *opinio juris*, and form a part of customary international law.

2. Adopting Special Emblems for Internet Infrastructure

Another option for heightening protection for internet infrastructure is to embrace a special protection regime based on emblems, such as the Red Cross or Blue Shield. As explained in the previous Part, emblematic protections and protections for medical workers illustrate that LOAC can be structured to provide special protections in cases for highly valuable objects, like humanitarian

workers in the battlespace. The emblem also recognizes the importance of creating a uniform system to distinguish specially protected persons and things. Internet access is not covered under existing humanitarian emblems. To establish a regime for protecting internet access, a new emblem could be crafted to safeguard physical internet infrastructure, such as critical routers, data storage centers, internet service providers, domain name registries, and cables.

Internet connectivity provides a host of essential humanitarian benefits. These warrant a level of protection similar to that accorded to aid workers and humanitarian observers. Indeed, the internet has been a very effective tool for the Syrian Observatory for Human Rights to illustrate the devastation and humanitarian plight of the Syrian civil war.[252] Additionally, internet access plays a huge role in modern culture and access to cultural symbols such as works of art, architecture, and science otherwise housed in museums. Beyond that, internet connectivity provides access to social connectivity, to loved ones, and to personally significant digital files, such as photographs, which maybe more treasured than any 'cultural property.' Just as humanitarian and cultural property enjoy special status in armed conflict, so too should internet connectivity.

Special emblem status under LOAC would provide additional protections and would cause military commanders and officials to think twice before terminating connectivity. Such status could be denoted by a distinctive mark, similar to the Blue Shield or Red Cross, which would be visible to belligerents. It would be placed on the rooftops and walls of facilities housing server farms and ISPs. Like Blue Shield-designated cultural properties, facilities housing internet infrastructure could only be targeted if shown to be aiding adversaries. Furthermore, the decision to attack would have to be made by senior military leaders, and all feasible precautions would need to be taken to minimize harm (such as attacking a cable connection outside, rather than the servers that house the civilian data)—adding substantial protections.

C. Employing Virtual Private Networks (VPNs) and Virtual Emblems to Enable Greater Military/Civilian Distinction in Digital Transmissions

A final proposal is to employ technology to make it easier to distinguish between military and civilian uses of the internet. States

252. SYRIAN OBSERVATORY FOR HUM. RTS,, https://www.whiteflagprotocol.org(last visited Jan. 11, 2021). The organization is widely cited as a source of ground-truth by journalists reporting on the conflict. *See, e.g., Syrian Observatory for Human Rights*, FIN. TIMES, https://www.ft.com/stream/55821138-8105-4f48-abad-09f718f0f6a5 (last visited Jan. 11, 2021).

and non-state combatants bear responsibility for putting the civilian internet at risk by co-utilizing it for military purposes. Under LOAC, parties are responsible for distinguishing between military and civilian objects through the wearing of uniforms and emblems. The principle of distinction also requires states not to locate military objectives near protected persons or institutions, such as hospitals or houses of worship.

However, protecting civilian internet connectivity in the digital world is much more challenging. Militaries use civilian internet infrastructure to transmit even secret communications,[253] rendering it vulnerable to targeting as a dual-use object. Further, internet transmissions are sent in packets of information, and come with varying layers of encryption making it challenging for even the best firewalls to separate civilian and belligerent communications. While parties might be forgiven for incorporating military communications onto the civilian internet in the past, now it is clear that too much is at stake—military and civilian internet uses should be separated.

Whereas physical emblems might protect internet infrastructure in the physical realm, virtual emblems and other technologies could do the same to distinguish humanitarian network traffic or applications. While developing a new separate military or civilian physical internet systems would be enormously costly, new technological advances allow for an affordable alternative: the creation of a 'virtual' separate network for special humanitarian functions that would enable 'highly protected' functions, such as humanitarian aid coordination, medical emergencies, and diplomatic correspondence. The technology behind virtual private networks (VPNs) has existed for decades and become mainstream, employing specific protocols (mainly encryption) to ensure privacy. Using the same programming, a protocol could be easily written that would flag certain networks, applications, or messages as humanitarian in nature. These might include emergency messages, prescription drug orders, health consultations, vital business transactions related to foodstuffs, and requests for assistance. Belligerents would be able to distinguish between humanitarian and military targets, which would enable them to enact blackouts which still permitted internet routing to transmit humanitarian communications. Under this system, belligerents would be able to review the messages and the underlying code unencrypted, to ensure it is not being abused. Additionally, this system could develop a specialized VPN exclusively for centers such as hospitals and pharmacies, so that if a belligerent caused a total blackout, these humanitarian-focused facilities would be spared.

253. Clark, *supra* note 64, at 234-37 ("classified military communications use the same network of submarine cables as civilian and unclassified data, making them susceptible to eavesdropping taps.").

A similar protocol has already been developed using blockchain technology to send secure and verifiable information between warring belligerents and humanitarian aid organizations.[254] The newly created Whiteflag Protocol enables entities protected under humanitarian law "to make themselves known in real-time to prevent collateral damage and casualties in conflict zones (deconfliction)."[255] It employs "blockchain, digital authentication, and encryption to secure messages and ensures the system remains neutral and cannot be controlled or manipulated, enabling a trusted global messaging/communications network."[256] Additionally, the blockchain records the history of events permanently and provides undeniable and transparent proof of the network's humanitarian activities.[257] Such technological developments illustrate that technological solutions may be available. While Whiteflag has been developed to share basic deconfliction information, its technology could be expanded upon to protect civilian internet access more broadly—thereby not merely allowing humanitarian organizations to share their locations, but fully facilitating civilian communications as well. Creating a trusted protocol for civilians to transfer digital data will help to distinguish civilian messages. This would create a digitally separate system by which humanitarian information could be passed. Perhaps systems, like pharmacy management or common internet ordering systems, could become verified trusted communicators enabling communications in formatted ways to prevent abuse, while allowing for vital civilian functions to still occur. This may provide a less costly way to preserve the most vital functions of the internet, while respecting the belligerents' potentially (if questionably) legitimate military goals in shutting down civilian internet access during war.

VII. CONCLUSION

Internet connectivity has become part of modern life and will become even more important in the future with the emergence of the 'internet of things' and AI. The COVID-19 pandemic further illustrates the vital importance of the internet during crises. Billions of people around the world rely on it for communications, business, health, education, and familial connection—it is a lifeline and the network that connects humanity. Surely it should enjoy special protection during armed conflict.

Currently, internet access enjoys strong explicit protection under IHRL, but does not enjoy similar status under LOAC or

254. WHITEFLAG PROTOCOL, www.whiteflagprotocol.org (last visited Aug. 17, 2020).

255. *Id.*

256. *Id.*

257. *Id.*

telecommunications law. LOAC, which applies *lex specialis*, does not offer a strong framework for protecting civilian internet connectivity. Despite the potential for harm to civilians, actions against internet access may not legally rise to the threshold of an 'armed attack,' which would justify the use of force under LOAC. Similarly, it may be difficult to assess scope and magnitude of civilian harm in a termination of internet connectivity under traditional LOAC proportionality analysis. Consequently, current LOAC seems insufficient to adequately safeguard the internet during armed conflict.

The global community should recognize the need for new norms and new laws. State practice and new international instruments should be implemented to specially recognize and protect civilian internet access during conflict. Adopting special emblems and explicit treaty safeguards, especially for submarine cables, would greatly improve the security of internet infrastructure during wartime. Such protections, coupled with adopting new virtual protocols to better separate military and civilian communications, would substantially improve protections offered under the current regime. The internet plays a vital role in modern society and must be protected, especially during conflict, to avoid intolerable human suffering.