KEYBOARD WARRIORS: HOW THE LAW OF ARMED CONFLICT MUST DEFINE THE DIFFERENCE BETWEEN CYBERWARFARE AND CYBERCRIME

GURNEY F. PEARSALL III*

ABSTRACT

This Article explores cybercrime, cyberwarfare, and how international law can better define and regulate these evolving digital threats. Cyberspace has rapidly become a critical domain for states and their citizens, so rapidly that the rules and norms of international law have not caught up. As a result, international law is unable distinguish between cybercrimes that justify police actions and acts of cyberwarfare that justify military action.

To close that dangerous, destabilizing gap in the law, this Article proposes a new approach. This Article argues that because cyberattacks and electromagnetic attacks share the same fundamental characteristics and often have indistinguishable battlefield effects, both tactically and strategically, they should, therefore, share the same international law framework.

* Mr. Pearsall practices family law with his sister at Pearsall Law Firm, PC. In addition, as a judge advocate in the US Army Reserve JAG Corps, he has had the honor of serving in national security law positions in the Pentagon, Fort Bragg, South Korea, and the Balkans. However, the views expressed in this Article are those of the author and do not represent the official policy or position of the US Government or any agency thereof, including the Department of Defense.

The author thanks Ann Van Hout and the editors of the *Wisconsin International Law Journal* for their valuable insights, and dedicates this Article to his son, Gurney F. Pearsall IV, whose expected delivery date is in July 2025!

https://doi.org/10.59015/wilj.KFTP9851

INTRODUCTION

Just after midnight on September 6, 2007, the cold, rocky desert of northeastern Syria rumbled as seventeen tons of bombs fell from the sky.[1] A handful of Israeli F-15 and F-16 strike fighters had cut across Syrian airspace, and turned a secret nuclear reactor into a smoldering hole in the ground.[2] One aspect of this air strike, known as Operation Orchard, continues to mystify experts: the Israeli planes could not hide from Syria's high-tech Russian air defense system, so how did it fail to spot them?[3]

In all likelihood, an electromagnetic (EM) attack or a cyberattack painted a false-sky picture across Syria's air defense system.[4] Either use of force would have had the same effect, yet there is a stark difference between EM attacks and cyberattacks in the eyes of international law. This difference in treatment has less to do with any substantive difference between the two uses of force, and more to do with the novelty of cyberspace. Electromagnetic warfare (EW) appeared on the battlefield in

---

[1] *See* Eric Lorber, *Executive Warmaking Authority and Offensive Cyber Operations: Can Existing Legislation Successfully Constrain Presidential Power?*, 15 J. CONST. L. 961, 969 (2013); *see also* David Makovsky, *The Silent Strike*, THE NEW YORKER, Sept. 17, 2012, at 34, 38.

[2] *See* Makovsky *supra* note 1, at 38; *see also* Thomas Rid, *Cyber War Will Not Take Place*, 35 J. STRATEGIC STUD. 5, 16 (2012).

[3] *See* Lorber, *supra* note 1.

[4] *See* Makovsky *supra* note 1, at 38.

1898, while the first large-scale, state-sponsored cyberattacks only began in 2007.[5] As a result, international law rules and norms have had ample time to address the legality of EM attacks, but they have had no time to address whether and to what extent international law applies to the new digital battlefield of cyberspace.

This Article proposes that because cyberspace operations and EM operations share the same fundamental attributes and battlefield effects, they should share the same international law framework. Until states adopt the clear-cut rules and norms of that framework, the legal grey zone around cyberattacks will pose a persistent, costly threat to US national security and to the national security of states around the world. State actors and non-state actors subject America's public and private sectors to a relentless fifteen thousand cyberattacks per year, costing billions of dollars and affecting the medical records, bank records, tax records, and other sensitive records of tens of millions of ordinary Americans.[6] Cyberattacks are growing in volume and intensity every year, and someday one will cause deaths. If that sounds like a far-away threat, the Department of Justice is already pursuing life sentences against two Sudanese men whose February 2023 cyberattack on a Los Angeles hospital redirected ambulances with patients away from emergency rooms, in an explicit effort to kill Americans.[7]

To clarify how states should be able to lawfully respond to such cyberattacks, this Article proceeds as follows. First, this Article overviews cyberspace and the history of cyberattacks in Part I. Part II discusses international law, the leading proposals for how international law should apply to cyberspace operations, and the flaws in those proposals. Part III explores the shared characteristics of cyberspace operations and EM

---

[5] *See* REBECCA RAINES, GETTING THE MESSAGE THROUGH: A BRANCH HISTORY OF THE U.S. ARMY SIGNAL CORPS 136 (1st ed. 1996) (stating that the U.S. Army's first field radios first saw action in 1898, during the Spanish-American War); *see, e.g.,* Marcel Hendrapati et al., *Qualifying Cyber Crime as a Crime of Aggression in International Law*, 13 J. E. ASIA & INT'L L. 397, 402 (2020) (discussing the cyberattack on Estonia).

[6] *See* Tom C.W. Lin, *Business Warfare*, 63 B.C. L. REV. 1, 27 (2022).

[7] *See* Andy Greenberg, *Hacker Charged with Seeking to Kill Using Cyberattacks on Hospitals*, WIRED (Oct. 16, 2024, 1:44 PM), https://www.wired.com/story/anonymous-sudan-ddos-indictment-takedown [https://perma.cc/3Y4H-L28G] (noting that the two men also carried out a cyberattack on October 7, 2023, within an hour of Hamas's large-scale attack, that disrupted Israel's ability to warn civilians of that incoming attack); *see Two Sudanese Nationals Indicted for Alleged Role in Anonymous Sudan Cyberattacks on Hospitals, Government Facilities, and Other Critical Infrastructure in Los Angeles and Around the World*, FLASHPOINT (Oct. 17, 2024), https://flashpoint.io/blog/usa-vs-ahmed-salah-yousif-omer-alaa-salah-yusuuf-omer/ [https://flashpoint.io/blog/usa-vs-ahmed].

operations, as exemplified by Operation Orchard, then proposes two legal frameworks that distinguish between cyberattacks that are crimes and cyberattacks that are acts of war.

I. A BRIEF HISTORY OF CYBERSPACE AND CYBERATTACKS

"Cyber" comes from the Greek word "kybernetes" which means governor or steersman.[8] This refers to computers because, ultimately, they are machines that carry out our instructions. These instructions can be as simple as typing an essay one letter at a time, or as complex as designing a large language model like ChatGPT, then asking it to predict what that essay should say.[9] As long as the instructions are executable and the computer has no malfunctions (or "bugs"), it will dutifully carry out its instructions.[10]

To execute these instructions, computers[11] need hardware and software.[12] "Hardware" refers to the computer's physical parts, such as the keyboard that types out instructions and the motherboard protecting most of the hardware.[13] "Software" is a computer's intangible parts.[14] Microsoft Word, for instance, is a software that lets ordinary people write documents without having to understand the intricacies of computer language.[15] Not all software programs are so helpful, however. Some carry out instructions *against* their users; this "malicious software" is known as "malware."[16]

---

[8] Maja J. Matarić, *The Robotics Primer* 8 (MIT Press, 2007).

[9] *See* Oluwatosin Ogundare & Gustavo Quiros Araya, *Comparative Analysis of ChatGPT and the Evolution of Language Models*, ARXIV (Mar. 28, 2023), https://arxiv.org/abs/2304.02468 [https://perma.cc/NUF5-G26V].

[10] Nicholas Bohm et al., *Briefing Note: The Legal Rule That Computers Are Presumed to Be Operating Correctly–Unforeseen and Unjust Consequences*, 19 DIGIT. EVIDENCE & ELEC. SIGNATURE L. REV. 123, 124–25 (2022).

[11] Bear in mind, "computer" is used in this Article in the broad sense, to include not only desktop computers and laptops but also phones, tablets, GPS devices, and the endless examples of smaller computers that we use in our day-to-day lives.

[12] Peter S. Menell, *Tailoring Legal Protection for Computer Software*, 39 STAN. L. REV. 1329 (1987), https://wwws.law.northwestern.edu/research-faculty/clbe/events/roundtable/documents/menell_tailoring_legal_protection_for_computer_software.pdf [https://perma.cc/T4ZA-8Q76].

[13] *See* Robert Plotkin, *Computer Programming and the Automation of Invention: A Case for Software Patent Reform*, 7 UCLA J. L. & TECH. 1, 26 (2003).

[14] *Id.* at 40.

[15] In fact, the Microsoft Corporation draws its name from the concept of a business that sells portable, micro software. *See* PAUL ALLEN, IDEA MAN 91, 104 (2011).

[16] Rabia Tahir, *A Study on Malware and Malware Detection Techniques*, 8 INT'L J. EDUC. & MGMT. ENG'G 20, 20 (2018).

Software, malware, and the myriad products that we create through them dominate the digital landscape known as cyberspace.

A cyberattack refers to the hostile use of cyberspace. Typically, a cyberattack involves gaining access to ("infecting") a computer through a vulnerability, then delivering a payload.[17] A cyberattack can target one very specific computer, or it can indiscriminately spread throughout cyberspace by infecting computers at random and self-replicating, like a virus.[18] This use of force may be new to the battlefield, but computer scientists have theorized about cyberattacks and computer viruses as far back as 1949.[19] By the 1970s, computer scientists created the first computer viruses in their computer labs.[20] But the first known cyberattack did not take place until 1981. That year, the first computer virus emerged in the wild, outside of a computer lab, and it came from a surprising source: a ninth-grade prankster in Pittsburgh.[21] His virus, called Elk Cloner, did nothing more than share a poem with the computers it infected.[22]

Most viruses deliver a far worse payload. For instance, the SCA Virus appeared six years later, spreading from computer to computer once an unsuspecting user inserted an infected floppy disc.[23] Upon infection, the malware executed a set of instructions that rendered games on the computer unplayable.[24] This affected roughly 40 percent of all computers in the Amiga family of personal computers, contributing to Amiga's downfall and the rise of its main competitor, Apple.[25]

---

[17] Lorber, *supra* note 1, at 977–78 (discussing each element in the vulnerability, access, payload framework).

[18] *See* JOHN VON NEUMANN, THEORY OF SELF-REPRODUCING AUTOMATA (1966) (publishing the 1949 lectures of John von Neumann, the "father of computer virology," delivered at the University of Illinois on the topic of "self-producing automata.").

[19] *See id.*

[20] Thomas M. Chen & Jean-Marc Robert, *The Evolution of Viruses and Worms*, *in* STATISTICAL METHODS IN COMPUTER SECURITY 265, 271 (2004) (discussing lab-created viruses such as the "Creeper" virus, an experimental computer virus that stalked ARPANET, the forerunner of the Internet, in the 1970s); *see also* Michael Gervais, *Cyber Attacks and the Laws of War*, 1 J. L. & CYBER WARFARE 8, 9 (2012) ("The first generation of malware in the 1970s was mostly experimental and did little damage beyond using computer memory and annoying its victims. When personal computing took hold in the 1980s, malware evolved into something more destructive. Viruses, worms, and other forms of malware spread quickly throughout the Internet, destroying data, overloading systems, and generally causing havoc."); *see also id.* at 11–17 (explaining how the Internet is a Cold War product, resulting from the U.S. government pouring money in ARPANET, as a way to continue communicating even after a nuclear apocalypse).

[21] Marcelo Triana, *Is Selling Malware a Federal Crime?*, 93 N.Y.U. L. REV. 1311, 1313–14 (2018).

[22] *See id.*

[23] Jimmy Maher, *The Future Was Here: The Commodore Amiga* 176 (MIT Press 2018).

[24] *Id.* at 174.

[25] *Id.*

A computer virus needs a host to spread, but cyberspace quickly evolved beyond that limit.[26] In 1988, a Cornell University student, Robert Morris, developed a malware that exists without a host, like a worm, simply to see if it was possible.[27] His malware, now known as the Morris Worm, visited websites and tested their passwords.[28] If the password was weak enough for the worm to correctly guess it, then the worm would enter into and remain on the website, like a squatter.[29] Websites can only support so much traffic before they slow down or freeze, but Morris was confident that one worm would make no noticeable difference.[30] To avoid infecting too many websites, he also ensured that only 14 percent of the worms would replicate themselves so that their clones could continue exploring the Internet's websites and passwords.[31]

Unfortunately, Morris forgot to prohibit the worm from reinfecting websites.[32] That minor oversight turned a harmless worm into a devastating one that severely slowed or even crashed websites under the weight of the sheer number of reinfections.[33] This quickly spiraled out of control, infecting about a tenth of all websites and costing up to $10 million to scrub from cyberspace.[34] Morris went on to earn the dubious honor of receiving the first conviction under the 1986 Computer Fraud and Abuse Act.[35] Of course, worms have, since then, grown far more sophisticated. For example, within fifteen minutes of infecting its first server in January 2003, the SQL Slammer Virus infected nearly half of the Internet's main servers, causing over $1 billion in damages before patches and antivirus software eliminated it.[36]

---

[26] For instance, SCA's infected floppy discs acted as a host. *See* NANCY E. MARION & JASON TWEDE, CYBERCRIME: AN ENCYCLOPEDIA OF DIGITAL CRIME 432 (2020).

[27] *See* Orin S. Kerr, *Norms of Computer Trespass*, 116 COLUM. L. REV. 1143, 1159 (2016); *see also* Chen & Robert, *supra* note 20, at 269. In all fairness, Robert Morris had not yet had the opportunity to hear the sage advice from Jeff Goldblum's character Ian, in Jurassic Park, released in 1993: "Your scientists were so preoccupied with whether or not they could, they didn't stop to think if they should." *See* Chris Lewis, *The Need for a Legal Framework to Regulate the Use of Artificial Intelligence*, 47 U. DAYTON L. REV. 285, 285 (2022) (quoting Jurassic Park but shortening "your scientists" to "they").

[28] *See* Kerr, *supra* note 27.

[29] *Id.* at 1160.

[30] United States v. Morris, 928 F.2d 504, 505 (2d Cir. 1991).

[31] *Id.* at 506.

[32] *See id.*

[33] *Id.*

[34] SAMUEL C. MCQUADE III, ENCYCLOPEDIA OF CYBERCRIME 123 (2008).

[35] *Morris*, 928 F.2d at 504.

[36] NEWTON LEE, COUNTERTERRORISM AND CYBERSECURITY: TOTAL INFORMATION AWARENESS 205 (2d ed. 2015).

A more recent cyberattack demonstrates that while cyberattacks and algorithms may be increasingly sophisticated, a cyberattack can still be effective, shocking, and targeted without any complicated malware—or, indeed, without any malware at all. In August 2014, a collection of about five hundred private photos of naked celebrities spilled across the Internet.[37] Apple investigated the matter and eventually discovered that the images were all taken from its online storage product, iCloud, in a cyberattack orchestrated by a thirty-six-year-old Pennsylvania man.[38]

That Pennsylvania man had engaged in a "phishing" campaign, fishing for sensitive information by sending out waves of personalized emails to celebrities and designing the emails to look like they had been sent by Apple itself.[39] The emails warned the victims of a potential security breach in their Apple account, then asked them to confirm their username and password.[40] Few of his targets responded, but for the ones that did respond, he was able to log into their iCloud account and download anything he could find.[41]

Jeff Bezos suffered a spyware attack in May 2018, after receiving a friendly text from his acquaintance, Saudi Crown Prince Mohammed bin Salman.[42] That text came with a piece of spyware known as Pegasus, resulting in his phone secretly transmitting enormous amounts of data back to Salman over the next few months.[43] While the attack took place in May 2018, it truly began in 2017, when the journalist Jamal Khashoggi began publishing a series of columns critical of Saudi Arabia in *The Washington Post*, which Bezos owned. *The Post* continued to vocally criticize the Saudi regime for luring Khashoggi into a Saudi embassy and murdering him. Without further ado, information about a secret extramarital affair

---

[37] *See* Christopher Satti, *A Call to (Cyber) Arms: Applicable Statutes and Suggested Courses of Action for the Celebrity iCloud Hacking Scandal*, 34 QUINNIPIAC L. REV. 561 (2016).

[38] *See* Andrew Blankstein, *Pennsylvania Man Is Charged in Celebrity Hack, Reaches Plea Deal*, NBC NEWS (Mar. 15, 2016), https://www.nbcnews.com/tech/tech-news/pennsylvania-man-arrested-will-plead-guilty-celebrity-hacking-n539166 [https://perma.cc/XY8L-CJAB].

[39] *See id.*

[40] *Id.*

[41] *Id.*

[42] *See* Anthony L. Fargo, *The End of The Affair: Can The Relationship Between Journalists and Sources Survive Mass Surveillance and Aggressive Leak Prosecutions?*, 26 COMM. L. & POL'Y 187, 204-05 (2021); Stephanie Kirchgaessner, *Jeff Bezos Hack: Amazon Boss's Phone Hacked by Saudi Crown Prince*, THE GUARDIAN (Jan. 22, 2020, 4:04 PM), https://www.theguardian.com/technology/2020/jan/21/amazon-boss-jeff-bezoss-phone-hacked-by-saudi-crown-prince [https://perma.cc/38G3-X4MK].

[43] *See* Kirchgaessner, *supra* note 42.

was forwarded from Bezos's phone to *The National Enquirer*.[44] Once published, the lurid tale of his affair quickly led to his $35 billion divorce.[45]

Despite how quickly viruses and worms began exploiting cyberspace, the first known, state-sponsored cyberattacks began decades later. In April 2007, Estonia removed a statue of a Soviet hero from a public park, over Russia's protests and threats.[46] The next day, and for the next roughly three weeks, websites for Estonia's government, banks, police, broadcasting organizations, and other important institutions crashed under the weight of a suddenly enormous volume of traffic.[47] Known as a Distributed Denial-of-Service (DDoS) attack, this sudden surge in traffic crashed Estonian websites in much the same way that a sudden surge of thousands of customers would overwhelm any store, even Walmart.[48] Such an attack could easily have become the first shots of an armed invasion.

The cyberattack on Estonia marks the first of many cyberattacks that blur the line between the world of cybercrimes and toward the world of armed conflict. While Estonia was fighting off DDoS attacks, the malicious Stuxnet worm was coursing through Iranian cyberspace, targeting thousands of computers involved in Iran's nuclear weapons program.[49] That infection began when someone inserted an infected flash drive into a computer connected to Iran's nuclear weapons program.[50] To this day, cybersecurity experts can only guess if the person was forced, tricked, or persuaded into spreading the infection, or if they simply broke into a facility and inserted it that way.[51]

Regardless of how or why the cyberattack began, Iranian officials failed to discover it until 2010, at which point it had already ruined about 20 percent of Iran's nuclear centrifuges and set back its nuclear ambitions

---

[44] *See id.*

[45] *Id.*

[46] *See* Hendrapati, *supra* note 5, at 402.

[47] *Id.*

[48] *See id.* at 415; *see also* Lorber, *supra* note 1, at 966–67 (describing the distributed denial of service attack).

[49] *See* Dorothy E. Denning, Stuxnet: What Has Changed? 4 FUTURE INTERNET 672, 676–82 (2012).

[50] Steven Cherry & Ralph Langner, *How Stuxnet Is Rewriting the Cyberterrorism Playbook*, IEEE SPECTRUM (Oct. 13, 2010).

[51] *Id.*

back by years, if not decades.[52] Upon infecting the computers that controlled the centrifuges, the Stuxnet Worm then instructed the computers to slowly overwork those centrifuges.[53] Meanwhile, the worm provided a false reading of normalcy to the nuclear scientists monitoring the machines.[54] No state has claimed responsibility over any of the aforementioned attacks, but cybersecurity experts assume that the Stuxnet worm was a joint American-Israeli creation and part of a larger cyber campaign known as Operation Olympic Games.[55] If so, Operation Olympic Games marks the first large-scale US-sponsored cyberattack.[56]

In 2015, Ukraine experienced its own Stuxnet-style malware attack. That December, a group of presumably Russian hackers used the BlackEnergy3 malware to target Ukrainian energy companies, resulting in a quarter million Ukrainians losing power for up to six hours in the dead of winter.[57] This marks the first time that a cyberattack caused a power outage, but it is just one of countless cyberattacks that have rocked Ukraine since Russia's 2014 invasion of its eastern region, the Donbas.

More recent armed conflicts echo Estonia's experience. Hours before Russia's invasion of Ukraine in 2022, a wave of DDoS attacks struck Ukrainian banking and defense websites, and hackers attacked the KA-SAT satellite network, cutting Ukrainian military communications.[58] Similarly, in the year leading up to Hamas's October 7, 2023, attack, Israel reported a 70 percent increase in Iranian cyberattacks.[59] Even on October 7 itself, within minutes of Hamas firing off its first volley of rockets, DDoS attacks disrupted Israel's ability to warn civilians about where the rockets were falling.[60]

---

[52] *See* Jay C. Jackson, Applying the U.S. and ICRC Standards for Direct Participation in Hostilities to Civilian Support of U.S. Military Operations, 92–94 (2018) (Masters of Laws Thesis, George Washington University).

[53] *See id.* at 50–52.

[54] *Id.*

[55] *Id.*

[56] *Id.*

[57] *See BlackEnergy Used as a Cyber Weapon Against Ukrainian Critical Infrastructure*, INFOSEC INSTITUTE (Jan. 4, 2016), https://www.infosecinstitute.com/resources/malware-analysis/blackenergy-used-as-a-cyber-weapon-against-ukrainian-critical-infrastructure/ [https://perma.cc/44JP-93R7].

[58] *Id.*

[59] Yoav Zitun, *IDF Says Iranian Cyberattacks Up 70% in 2022*, YNETNEWS (Jan. 2, 2023), https://www.ynetnews.com/article/r1cn9odzj [https://perma.cc/V9XJ-S2JT].

[60] Omer Yoachimik & Jorge Pacheco, *Cyber Attacks in the Israel-Hamas War*, THE CLOUDFLARE BLOG (Oct. 23, 2023), https://blog.cloudflare.com/cyber-attacks-in-the-israel-hamas-war/ [https://perma.cc/JX95-AQ9].

Going forward, the complexity, cleverness, and persistence of both types of cyberattacks is bound to continue growing. While the attacks themselves grow at an exponential pace, their goals will likely remain the same. Russian cyberattacks generally aim to sow discord in and unravel the societies of Western states.[61] Chinese spyware cyberattacks typically focus on stealing intellectual property from Western states, thus saving a fortune on research and development for advanced technology.[62] North Korea relies on ransomware cyberattacks to raise hard currency.[63] Meanwhile, American and Israeli cyberattacks tend to support or act as a substitute for conventional uses of armed force.[64]

Clearly, cyberattackers wield a vast arsenal of sophisticated tools, tactics, and strategies, and a wide variety of motivations drive their cyberattacks. But this brief, simplified overview should help clarify what cyberspace is, how it has rapidly evolved, and why both non-state actors and state actors weaponize it. When non-state actors launch cyberattacks, victim states often take action, treating it as a cybercrime for law enforcement officers to deal with.[65] But when states launch the same kinds of cyberattacks, victim states rarely take action against the state sponsor.[66] This muted response gives states all the more reason to continue using cyberspace as a weapon and intensifying the breadth and depth of their cyberattacks. To add some much-needed clarity to this area of international law, and thus reduce the scope and intensity of armed conflict, Part II explores how the law of armed conflict should more clearly distinguish between cybercrimes and cyberwarfare.

---

[61] Tom C.W. Lin, *Business Warfare*, 63 B.C. L. REV. 1, 29–30 (2022); Jon M. Garon, *Cyber-World War III: Origins*, 7 J.L. & CYBER WARFARE 1, 4–5 (2018).

[62] *See id.* at 15–17.

[63] *Id.* at 18–19.

[64] *See* Gary D. Brown & Owen W. Tullos, *On the Spectrum of Cyberspace Operations*, SMALL WARS J., 5 (Dec. 2012).

[65] *See, e.g.* Greenberg*, supra* note 7 (the arrest and prosecution of Robert Morris and the two brothers who attacked Los Angeles hospitals illustrate how the U.S. has not hesitated to seize and prosecute non-state actors for cyberattacks).

[66] For example, in response to state-sanctioned cyberattacks, the US typically does little more than punish private individuals and private companies instead of government officials or government agencies. Only in the most extreme cases has a US president directly sanctioned a state for cyberattacks, by expelling diplomats, closing consulates, and sanctioning government agencies. *See* Exec. Order No. 13,757, 82 Fed. Reg. 1 (Dec. 28, 2016) (sanctioned Russian government agencies, intelligence services, and companies linked to recent cyberattacks against the US); Exec. Order No. 14,024, 86 Fed. Reg. 20249 (Apr. 15, 2021) (expanding US sanctions against Russian individuals and government agencies for continued cyberattacks, election interference, hacking, and disinformation campaigns).

II. CYBERSPACE OPERATIONS AND INTERNATIONAL LAW

It may sound hyperbolic to suggest that a state would ever respond to a cyberattack with military force, but it has already happened. On May 5, 2019, Hamas's cyber unit launched a wave of cyberattacks on Israeli military targets.[67] Israeli cybersecurity personnel soon pinpointed the source of the attack to a building in Gaza, and the resulting air strike marks the first time a state has used conventional armed force in response to a cyberattack.[68]

Was that air strike a lawful act of self-defense or was it a violation of international law? When can states use military force in response to cyberattacks? For some international law scholars, the answer is *never*. They argue that the very concept of "cyberwarfare" needlessly militarizes cyberspace, and that cyberattacks may be crimes or acts of espionage, but they are never acts of war.[69] Unfortunately, the militarization of cyberspace has already taken place. It is hard to characterize it as anything less than "militarized" when state armed forces have dedicated cyberwarfare units, using cyberspace both tactically, in operations such as Operation Orchard, and strategically, in military campaigns such as Russia's invasion of Georgia and Ukraine.[70] Cybercrimes come from individuals acting for their own benefit, with no connection to any armed conflict, but with cyberwarfare, states directly sponsor and participate in

---

[67] Elias Groll, *Report: The Future Is Here, and It Features Hackers Getting Bombed,* FOREIGN POLICY (May 6, 2019, 7:36 PM), https://foreignpolicy.com/2019/05/06/the-future-is-here-and-it-features-hackers-getting-bombed/ [https://perma.cc/PM9U-MEX7] (discussing the hacking campaign and air strike, and a 2015 air strike by US forces against an ISIS hacker).

[68] *Id.*

[69] Ron Deibert, *Tracking the Emerging Arms Race in Cyberspace*, 67 BULLETIN OF THE ATOMIC SCIENTISTS 1 (2011); Ryan Singel, *White House Cyber Czar: "There Is No Cyberwar,"* WIRED (2010), https://www.wired.com/2010/03/schmidt-cyberwar/ [https://perma.cc/PL7K-9TLA] (quoting Howard Schmidt, former Cyber Security Coordinator of the Obama Administration, as stating that "there is no [such thing as] cyberwar. . .I think that is a terrible metaphor and I think that is a terrible concept. There are no winners in that environment.").

[70] Garon, *supra* note 61, at 3–18; Lorber, *supra* note 1, at 965–69; Gervais, *supra* note 20, at 42 ("As mentioned, many states have already begun developing cyber units within their military or intelligence apparatuses. States have also delegated some elements of their cyber attack capabilities to the private sector. One state might even consider using another state to launch an attack on its behalf. Although tracing a cyber attack is a formidable technical challenge, if the target state successfully traces a cyber attack to the source state's cyber unit or to an entity acting with the authority or under the control of the source state, the latter ought to be held responsible.").

hostilities.[71] International law must, therefore, reflect the reality that cyberspace, like airspace, can be thoroughly militarized.[72]

International law is made up of treatises and unwritten norms, covering human rights law, economic relations, diplomatic immunity,

---

[71] Duncan B. Hollis, *Why States Need an International Law for Information Operations*, 11 LEWIS & CLARK L. REV. 1023, 1026 (2007) ("Estonia's Defense Minister Jaak Aviksoo insisted that such sabotage 'cannot be treated as hooliganism, but has to be treated as an attack against the state.' As Estonia's Defense Ministry Spokesperson explained, 'If you have a missile attack against, let's say, an airport, it is an act of war. . . .If the same result is caused by computers, then how else do you describe that kind of attack?'"). In addition, in its February 2010 study of emerging threats to national security, the United States Joint Forces Command included a lengthy review of cyberspace threats, stating:

> With very little investment, and cloaked in a veil of anonymity, our adversaries will inevitably attempt to harm our national interests. Cyberspace will become a main front in both irregular and traditional conflicts. Enemies in cyberspace will include both states and non-states and will range from the unsophisticated amateur to highly trained professional hackers. Through cyberspace, enemies will target industry, academia, government, as well as the military in the air, land, maritime, and space domains. In much the same way that airpower transformed the battlefield of World War II, cyberspace has fractured the physical barriers that shield a nation from attacks on its commerce and communication. Indeed, adversaries have already taken advantage of computer networks and the power of information technology not only to plan and execute savage acts of terrorism, but also to influence directly the perceptions and will of the U.S. Government and the American population.

U.S. JOINT FORCES COMMAND, THE JOINT OPERATING ENVIRONMENT 34–36 (2010).

[72] Peter C. Combe II, *Traditional Military Activities in Cyberspace: The Scope of Conventional Military Authorities in the Unconventional Battlespace*, 7 HARV. NAT'L SEC. J. 526, 530-33 (2016) ("Covert activities are unacknowledged actions by the United States Government that are undertaken to 'influence political, economic, or military conditions abroad.' Such activities are subject to formalistic decision-making and oversight rules. The President or Secretary of Defense must approve all covert activities that are not in support of ongoing hostilities. Furthermore, the executive must provide detailed reports on covert activities to the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence."); *see also* Alexandra H. Perina, *Black Holes and Open Secrets: The Impact of Covert Action on International Law*, 53 COLUM. J. TRANSNAT'L L. 507, 512 (2015) ("Covert acts are generally conducted so as to create 'plausible deniability,' though to be sure mechanisms of obscuring attribution are not always effective. Covert actions discussed herein are unacknowledged operations intended to influence events in another country, conducted by any state agency or actor, or other entity acting on behalf of a state. This generic sense of 'covert' is largely consistent with but slightly broader than the U.S. statutory definition of 'covert action.' The National Security Act defines covert action as 'an activity or activities of the U.S. Government to influence political, economic, or military conditions abroad, where it is intended that the role of the U.S. Government will not be apparent or acknowledged publicly,' excluding certain categories of government conduct such as intelligence gathering and traditional diplomatic, military, or law enforcement activity. Though the term 'clandestine' is often colloquially used interchangeably with 'covert,' the U.S. military defines 'clandestine' to mean a military operation designed so as to conceal the operation itself. Clandestine, unacknowledged traditional military activities that fall outside the U.S. statutory definition of covert action could be 'covert' conduct of interest to this study.").

armed conflict, and myriad other topics.[73] The law of armed conflict (LOAC) bears the most relevance to the question of when a cyberattack is serious enough to create an armed conflict.[74] What would make a digital attack "armed"? For that matter, what makes any conflict an "armed" conflict?[75]

That question weighed heavily on the drafters of the UN Charter. The drafters found themselves torn between creating a charter that banned either all conflict or only armed conflict. Clearly, the drafters of Article 2(4) preferred the broader mandate for the UN.[76] To this day, Article 2(4) still bans states from using any force: "All [UN] Members shall refrain in their international relations from *the threat or use of force* against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."[77] The one exception to this ban comes from Article 51, which allows states to use armed force when defending themselves or when expressly authorized by the UN Security Council.[78]

But that constitutes a minority opinion. The majority of the drafters and delegates ultimately preferred the narrow mandate, banning only armed force, which is why Article 41 allows states to use certain kinds of unarmed force, such as the "complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communication, and the severance of diplomatic relations."[79] Of course, embargoes, tariffs, sanctions, diplomatic isolation, and the many

---

[73] Valentina Vadi, *International Law and Its Histories: Methodological Risks and Opportunities*, 58 HARV. INT'L L. J. 311 (2017).

[74] LOAC is sometimes more colloquially referred to as the Law of War. But because these doctrines apply to even low intensity conflicts, and not just to large-scale combat operations, the more accurate term would be Law of Armed Conflict. The term "International Humanitarian Law" is also synonymous with LOAC. In the author's experience, newcomers to this area of law tend to conflate the terms "International Humanitarian Law" and International Human Rights Law, which are distinct international law doctrines.

[75] A similar question loomed over the Guantanamo Bay cases. During the oral arguments for a habeas corpus proceeding for the Guantanamo Bay detainee Yaser Hamdi, Justice Sandra Day O'Conner pressed the solicitor general to define "combatant," since the government alleged that Hamdi was an enemy combatant. He responded with the famously unsatisfactory definition that a combatant is "one [who is] taking part in combat." Transcript of Oral Argument at 6, Hamdi v. Rumsfeld, 542 U.S. 507 (2004) (No. 03-6696), https://www.supremecourt.gov/oral_arguments/argument_transcripts/2003/03-6696.pdf [https://perma.cc/M65F-EMGL].

[76] Matthew C. Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, 36 YALE J. INT'L L. 421, 427–28 (2011).

[77] U.N. Charter art. 2, ¶ 4.

[78] *Id.* at art. 51.

[79] *Id.* at art. 41.

other kinds of activities permitted under Article 41 are often far more devastating than any air strike. But, as far as the UN Charter is concerned, those options at least offer a more peaceful alternative to armed conflict.

In *Nicaragua v. United States*, the International Court of Justice has long since established that because Article 41 permits the use of economic, political, and other kinds of unarmed force, Article 2(4) cannot mean what it literally says.[80] Despite its literal meaning, then, Article 2(4)'s plain meaning is to prohibit only armed force.[81] *Nicaragua*'s framework clarifies that, as far as international law is concerned, cyberattacks (like any other attacks) either involve armed or unarmed force, with sanctions, embargoes, and diplomatic isolation offering examples of "unarmed" force.[82]

Still, what is "armed" about armed force? Is there ever anything "armed" about a digital attack? Cyberattackers may wield a vast arsenal of tools, but none of those tools are cruise missiles, assault rifles, or any other conventional weapons of war. The UN Charter discusses armed force without defining it, so *Nicaragua* goes on to define it. To better understand that definition, we must better understand *Nicaragua*'s context. *Nicaragua* involved Cold War politics, with the USSR providing military aid, economic assistance, and political backing to the socialist Sandinista government, a Marxist group that overthrew Nicaragua's right-wing capitalist government in 1979, and the US providing funding, training, weapons, and logistical support to the Contras, a right-wing and anti-communist group.[83] While arming the Contras, US armed forces also mined Nicaragua's harbors and conducted intelligence and reconnaissance operations into Nicaragua.[84]

In 1984, Nicaragua filed a case against the US at the International Court of Justice, accusing the US of violating its sovereignty and engaging in acts of aggression, in violation of UN Charter Article 2(4).[85] In response, the US argued that the court lacked jurisdiction and, more importantly, that its acts constituted the lawful exercise of collective self-defense.[86] The US argued that its aggressions were a lawful response to

---

[80] Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, ¶¶ 191–93 (June 27).

[81] *Id.*

[82] *Id.*

[83] *Id.* at ¶¶ 228–31.

[84] *Id.*

[85] *Id.* at ¶ 1.

[86] *Id.* at ¶¶ 26, 223–35.

Nicaraguan aggressions, as the Nicaraguan government was supporting and arming leftist insurgents in its neighboring territories.[87]

To draw a clearer line between armed and unarmed force, *Nicaragua* defines "armed" force as the use of military weapons or personnel to cause physical harm.[88] By that definition, the US engaged in armed force by laying mines in Nicaragua's harbors, which harmed Nicaragua by obstructing its maritime navigation and damaging several commercial and civilian vessels.[89] Laying mines in harbors is far from the unarmed, passive embargo that Article 41 permits. Similarly, the court found that US support for the Contras also constituted armed force because the support (arming, training, and supplying) directly enabled their military operations against Nicaragua.[90] By contrast, even if the US had presented conclusive evidence that Nicaragua funded neighboring insurgents, that level of support would not have been significant enough, on its own, to directly enable military operations.[91]

This definition of "armed" offers a framework for cyberattacks as well. The *Nicaragua* court had mines and grenades in mind when it discussed the use of military weapons, but international law recognizes that dual-use items such as cars and knives—and, arguably, computers—become weapons of war when they are in the hands of combatants or when used for military purposes.[92] This is why an armed use of force takes place if a state or an organized armed group (for example, a group of insurgents) uses anything, even cyberspace, in a manner that physically harms people or property, in violation of another state's territorial sovereignty.[93]

For example, the Morris Worm would not meet this definition because, while it caused significant disruption to computer networks in states all over the world, it caused only reversible, temporary inconveniences and financial losses instead of any physical harm. In addition, the inconveniences that Morris caused resulted from his failure to understand what his code would do, not from any intentional or targeted attack. By contrast, the Stuxnet Worm deliberately attacked and significantly damaged a large portion of Iran's nuclear program. As a

---

87 *Id.* at ¶¶ 223–35.

88 *Id.* at ¶ 195.

89 *Id.* at ¶¶ 228–29.

90 *Id.*

91 *Id.*

92 YORAM DINSTEIN, THE CONDUCT OF HOSTILITIES UNDER THE LAW OF INTERNATIONAL ARMED CONFLICT 84–86 (3d ed. 2016).

93 *Id.*

result, that attack would more likely constitute an armed use of force, albeit digital force.

Nicaragua sheds light on one final key question about the role of cyberattacks in LOAC, namely: the UN Charter permits the use of armed force in self-defense, but to what extent? If a state experiences a Stuxnet-style attack, then is that victim state free to respond with an all-out invasion, or does the UN Charter impose some limit on the victim state's right to fight back in self-defense? To answer this, *Nicaragua* noted that the UN Charter's prohibitions repeatedly, and without explanation, shift language between "armed force" and "armed attack." For example, Articles 2(4) and 41 ban "armed force," but Article 54 bans "armed attack." Some would dismiss that difference as meaningless semantics, but the court found that these words mean very different things, by creating two very different levels of severity.[94]

Specifically, the court ruled that an "armed attack" is a grave use of force involving coordinated violence of substantial scale or gravity, while "armed force" is any armed force.[95] The threshold for armed force is remarkably low: whether a battalion of one thousand soldiers cross the border in a large-scale raid, or just one soldier drunkenly stumbles across the border in search of a fistfight, armed force is at play.[96] LOAC applies to either incident, in order to maximize the protective coverage that LOAC affords to combatants and noncombatants alike.[97]

While LOAC applies to both incidents, *Nicaragua* ruled that the right to use armed force in self-defense only applies in the case of an armed attack.[98] As such, states have wide discretion in how to use military force in response to an invasion, air strike, or even a small raid. But, in response to a more trivial use of armed force, the right to use force in self-defense would not apply. Instead, the UN Charter expects states to apply unarmed

---

[94] *See* E. Wilmhurst, *Principles of International Law on the Use of Force by States in Self-Defense*, Chatham House (Oct. 1, 2005), https://www.chathamhouse.org/sites/default/files/publications/research/2005-10-01-use-force-states-self-defence-wilmshurst.pdf [https://perma.cc/K7YH-WVAX] (advocating the minority viewpoint that any use of armed force constitutes a *per se* armed attack); *Nicar. v. U.S.*, *supra* note 80, at ¶ 191.

[95] *Nicar. v. U.S.*, *supra* note 80, at ¶ 195; Laurie R. Blank, *Irreconcilable Differences: The Thresholds for Armed Attack and International Armed Conflict*, 96 NOTRE DAME L. REV. 249, 261–62 (2020).

[96] Blank, *supra* note 95, at 260 ("The threshold for international armed conflict is therefore 'remarkably low'–one airstrike, detention of one soldier, even an incursion onto the adversary's territory without consent is sufficient.").

[97] *Id.* at 261–62.

[98] *Id.*

"countermeasures."[99] For example, if State A's border guard crosses into State B's border, State B should treat it as a civil matter for police forces to handle, not as a military matter for the victim state to violently escalate. Instead, State B may detain the guard as a trespasser, offer diplomatic protests, suspend cooperation agreements with State A, impose sanctions on State A, and/or engage in some other unarmed type of force. State B may not use the incident as pretext to launch an all-out war. More serious threats may require a military response, as a matter of military necessity, but that response must still do nothing more than neutralize an immediate threat and regain territorial sovereignty.[100]

Released in 1984, the *Nicaragua* case came long before the militarization of cyberspace. So, while it provides a helpful framework for defining the distinction between unarmed force, armed force, and armed attacks, it offers no guidance for how to understand whether something as peculiar as a cyberattack could ever rise to the level of an armed attack. To date, the International Court of Justice has released no rulings or advisory opinions about cyberattacks. To fill this gap, three schools of thought have emerged, arguing that this "armed attack" determination for cyberattacks should depend on the target, the method of attack, or the effects of the attack.

A. TARGETING AS THE BASIS OF THE CYBERCRIME/CYBERWARFARE DISTINCTION

The target-oriented school of thought stretches back as far as 1999.[101] Under a simplistic targeting theory of legality, cyberattacks against civilians are cybercrimes, while cyberattacks against government and military targets are acts of armed force. Most proponents in this school of thought prefer a more nuanced approach, arguing that it is only an act of armed force if the cyberattack targets critical national infrastructure.[102] "Critical national infrastructure" is a broad category, and scholars often disagree about how broadly to define it. Generally, it includes electric power grids, nuclear power plants, and other physical or non-physical

---

[99] Int'l Law Comm'n, Rep. on the Work of Its Fifty-Third Session, U.N. Doc. A/56/10, at 129 (2001) (codifying customary international law on countermeasures and specifying that while states may take countermeasures against internationally wrongful acts, these acts must be proportional to the threat and must avoid the use of armed force).

[100] Hendrapati, *supra* note 5, at 412–13.

[101] WALTER GARY SHARP, SR., CYBERSPACE AND THE USE OF FORCE 129–32 (1999).

[102] *Id.*

systems essential for maintaining government operations and the basic functioning of society.[103]

The targeting-oriented approach to classifying cyberspace operations establishes a relatively clear line for would-be cyberattackers. This line puts them on notice of what cyberattacks may result in police action, and what cyberattacks may result in military action. If this deters some attacks on government targets, military targets, or critical national infrastructure, then it has accomplished LOAC's foundational goal of reducing the scope and intensity of armed conflict.[104]

But a targeting-based theory of classification sharply diverges from the usual LOAC analysis.[105] Should a tank fire a shot across the border, for example, that is unquestionably a use of armed force, no matter what the tank was aiming at or ends up hitting.[106] Why should it matter what the tank was targeting? Arguably, it makes no difference what the tank targeted because the tank crew is not made up of civilians, who can be arrested by the victim state's police forces for firing the shot across the border. But as far as LOAC is concerned, even if a group of civilians commandeer a tank and start shooting across an international border, LOAC still applies and they are still lawfully targetable by the victim state's military forces for as long as they continue to directly participate in hostilities.[107] This is true no matter what their targets may be.[108]

---

[103] *Id.*

[104] United States v. Al Bahlul, 820 F. Supp. 2d 1141, 1188 (USCMCR, 2011) ("Terrorism is, above all, the negation of law. More specifically, it is the negation of the fundamental humanitarian principles of the law of armed conflict. Whereas humanitarian law proscribes directing attacks against civilians as such, terrorism promotes it; and whereas a fundamental purpose of jus in bello is the facilitation of order after a conflict, the aim of terrorism is the opposite - chaos clad in violence. . . .Application of the law of armed conflict, and in particular its bedrock principles of distinction and fundamental protections, serves humanitarian ends and ultimately reinforces the rules governing international behavior at all times, even in war").

[105] Blank, *supra* note 95, at 261–62.

[106] *Id.*

[107] Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), art. 51(3), June 8, 1977, 1125 U.N.T.S. 3 (Stating that non-combatants lose protection from intentional armed attack "for such time as they take a direct part in hostilities.").

[108] Nils Melzer, *Interpretive Guidance on the Notion of Direct Participation in Hostilities Under International Humanitarian Law*, INT'L COMM. OF THE RED CROSS (2009), https://www.icrc.org/en/doc/assets/files/other/icrc-002-0990.pdf [https://perma.cc/3JJU-SWJD] ("The use of weapons or other means to commit acts of violence against human and material enemy forces is probably the most uncontroversial example of direct participation in hostilities," which highlights the fact that the person, place, or thing in the civilian's crosshairs is not the issue; the issue is that the civilian is shooting in the first place).

Another argument might be that there is, or at least should be, a unique LOAC rule for classifying cyberattacks because they are non-kinetic. But why should that unique LOAC rule for cyberattacks not apply to the many other types of non-kinetic action, such as EM attacks or blockades, both of which fall under the usual rules and norms of armed conflict? If State A blockades State B ports or uses jammers to shut down even just a portion of State B's air defense system then, under *Nicaragua*'s use-of-force framework, State A is using armed force, potentially enough armed force to constitute an armed attack. The usual LOAC rules and norms would apply to that armed conflict. Why should LOAC treat this same non-kinetic scenario any differently if State A instead unleashes a Stuxnet-like attack that shuts down State B ports, or an Operation Orchard-style attack that shuts down State B's air defense system? There is nothing about the non-kinetic nature of these attacks that should immunize them from the usual rules and norms of war.

B. METHOD OF ATTACK AS THE BASIS OF THE CYBERCRIME/CYBERWARFARE DISTINCTION

A smaller school of thought proposes that the legality of cyberattacks should depend on how an attack unfolds.[109] This theory argues that certain kinds of cyberattacks are so inherently destructive or disruptive as to be the legal equivalent of bullets and bombs.[110] But, in practice, this approach fits cyberspace operations even more poorly than the target-oriented approach. Any kind of cyberattack can wreak havoc. The Morris Worm, SQL Slammer Virus, and Apple iCloud Hack were all enormously destructive and disruptive, but few would argue that they were acts of war that justified an air strike. In addition, any kind of cyberattack can fizzle out with little to no effect.

By contrast, every use of chemical, biological, and nuclear weapons is inherently extremely destructive. Meanwhile, the Stuxnet Virus harmed no one and affected hardly anyone, but it is clearly the result of one or more states using cyberspace as a weapon and destroying important military targets in the process. In practice, the method-of-attack

---

[109] Charles J. Dunlap Jr., *Perspectives for Cyber Strategists on Law for Cyberwarfare*, 5 STRATEGIC STUDIES QUARTERLY 81, 84 (2011) (proposing that any attack conducted through cyberspace methods is, at most, a cybercrime, like any other state-sponsored acts that constitute international criminal offenses instead of acts of war).

[110] *See id.*

school of thought offers a poor doctrinal fit for how to decide when cyberattacks are severe enough to constitute an armed attack.

C. EFFECTS AS THE BASIS OF THE CYBERCRIME/CYBERWARFARE DISTINCTION

The most popular proposal is the effects model. Under this model, if a cyberattack results in the same kind of effects as an armed attack, then it is an armed attack. The Tallinn Manual on the International Law Applicable to Cyber Warfare encapsulates this school of thought.[111] The Manual recommends that cyberattacks fall under LOAC when they are "reasonably expected to cause injury or death to persons or damage or destruction to objects."[112]

Drawing a line at injury, death, damage, and destruction brings the effects of a LOAC cyberattack closer to the effects inherent to most conventional weapons. Pinning the offense to what the parties reasonably expect is, of course, bound to result in endless debate about the reasonableness of one expectation or another. But even a narrower definition that focuses more objectively on injury, death, damage, and destruction would have two fundamental problems.

First, no cyberattack has ever directly resulted in injury or death. If someone intends to inflict injury or death, firearms and explosives are easier to access, simpler to learn, and far more likely to directly achieve those goals than malware. Even for damage or destruction, cyberattacks only achieve such results indirectly, after the targeted computer system carries out its malicious instructions. The effects of an EM attack—for instance, an attack that fries a circuit board upon impact—are more comparable to the effects of, say, a bomb going off. Because cyberattacks rarely result in the kind of effects closely associated with armed conflict, this model of classification gives carte blanche to a vast array of cyberattacks that significantly threaten national security but cause no damage, such as spyware attacks and ransomware attacks.

Second, even for cyberattacks whose physical effects are incomparable to those of conventional attacks, the tactical or strategic effects between cyberattacks and conventional attacks are often

---

[111] *See* MICHAEL N. SCHMITT, TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (1st ed. 2013) (Tallinn Manual); MICHAEL N. SCHMITT, TALLINN MANUAL ON INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS, (2nd ed., 2017).

[112] *See* Schmitt, *supra* note 111, at Rule 92.

indistinguishable.[113] By destroying 20 percent of Iran's nuclear centrifuges in one strike, the Stuxnet Virus effectively carried out a strategic bombing campaign, without ever putting any life at risk. With Iran now building nuclear weapons research facilities so far underground that no bomb can reach them, a cyberweapon may be the only weapon left.[114] By painting a false-sky picture across Syria's air defense system, Operation Orchard temporarily destroyed Syria's air defense system, without raising any alarms or causing any injury, death, or damage. Spyware is effectively a type of espionage. Like most forms of wartime espionage, spyware damages nothing and harms no one. Why, then, should it not be treated as espionage?

Clearly, as much of a step forward as the effects model may be, its inapplicability to cyberspace operations is still substantial enough to make it a poor international law standard. Part III offers a stronger standard and explores why drawing LOAC rules and norms of cyberspace operations from those of EW avoids the many pitfalls and inconsistencies identified above.

III. ELECTROMAGNETIC WARFARE AS A MODEL FOR CYBERSPACE

The closest model to cyberspace is EW. Like most cyberattacks, most EM attacks are non-kinetic, and both cyberattacks and EM attacks focus on disabling or degrading systems and signals.[115] But, unlike the almost nonexistent legal framework for cyberspace, the legal framework for EM attacks has had well over one hundred years to develop.[116] To better understand that context, this Part briefly overviews that development.

---

[113] Tobias Kliem, *You Can't Cyber in Here, This is the War Room! A Rejection of the Effects Doctrine on Cyberwar and the Use of Force in International Law*, J. ON THE USE OF FORCE AND INT'L. L. 344, 349 (2017).

[114] Jon Gambrell, *An Iranian Nuclear Facility is So Deep Underground That US Airstrikes Likely Couldn't Reach It*, AP NEWS (10:40AM, May 22, 2023), https://apnews.com/article/iran-nuclear-natanz-uranium-enrichment-underground-project-04dae673fc937af04e62b65dd78db2e0 [https://perma.cc/ESW8-M5GN].

[115] Jair Aguirre et al., *Scaling Non-Kinetic Capability Integration in the Information Age*, RAND CORPORATION (2024), https://www.rand.org/pubs/research_reports/RRA1934-1.html [https://perma.cc/NR2A-WGL9].

[116] CHRISTOPHER H. STERLING, MILITARY COMMUNICATIONS: FROM ANCIENT TIMES TO THE 21ST CENTURY (1st ed., 2007).

On the first battlefields, commanders carried out tactical communications by shouting.[117] As battlefields grew larger and louder, commanders began resorting to musical instruments for auditory cues or flags for visual cues; eventually, they resorted to runners on horseback.[118] By the nineteenth century, battlefields had grown so large that even communication by horseback led to long delays between issuing and receiving orders—assuming that the runner ever even delivered the message, considering the risk of death or capture along the way.[119] With the invention of the radio, the electromagnetic spectrum (EMS) suddenly brought back the voice commands of a long gone era.[120] By 1898, US Army commanders in the Spanish-American War were directing troops by radio.[121]

But just as combatants can capture runners on horseback or overhear verbal commands, so too can they intercept radio communications. Radio communications travel along certain frequencies and remain audible to anyone listening in on those frequencies.[122] Not only can those eavesdroppers hear the radio communication, but they can also make their own noise on that frequency, even to the point of drowning out any understandable communication.[123] In other words, overloading a frequency with noise would render that part of the EMS useless to enemy and allied forces alike.[124] This use of the EMS for offensive purposes is known as "jamming," and it marks the beginning of EW.[125]

During the 1904–1905 Russo-Japanese War, a Japanese auxiliary cruiser located a Russian fleet and began radioing information about its location back to the Japanese fleet.[126] A Russian naval captain requested permission to blast radio signals at the Japanese ship to distort its radio transmissions.[127] His superior denied this request, failing to comprehend

---

[117] Raines, *supra* note 5, at 3.

[118] *Id.* at 5.

[119] *Id.* at 3.

[120] *Id.* at 172.

[121] *Id.* at 105.

[122] *See generally* Vincent L. Defabo, *Rethinking Cyberspace Operations: Widespread Electromagnetic Jamming by States Indicates Cyber Interference is Not a Use of Force*, 86 J. AIR L. & COM. 219, 224–26 (2021).

[123] *Id.* at 226.

[124] *Id.*

[125] *Id.*

[126] STERLING, *supra* note 116.

[127] *Id.*

how blasting signals could stop enemy communications.[128] As a result, the Japanese fleet located and decisively destroyed the Russian fleet during the Battle of Tsushima.[129]

Since then, the EMS has become a critical domain for commercial and military purposes alike.[130] Many, if not all, of the most important systems in high-tech countries are now spectrum dependent. Every year, more dams, bridges, and other pieces of critical national infrastructure are hooked up to a computer for observation and control.[131] Like cyberwarfare, EW extends the range of military operations beyond the traditional air, land, sea, and space domains. With EW, the range of military operations now includes the EMS.

Unlike cyberspace, the EMS is not a human creation; it exists independently of any human involvement.[132] The EMS's many oscillating electric and magnetic wavelengths and photon energies are organized by frequency, ranging from less than one hertz to over one trillion hertz.[133] These frequency ranges are themselves divided into bands.[134] From the longest wavelengths and lowest frequencies to the shortest wavelengths and highest frequencies, these bands are known as radio waves, microwaves, infrared, visible light, ultraviolet, X-rays, and gamma rays.[135]

EW involves the use of the EMS or directed energy on a target.[136] Typically, the goal is to either protect one's own spectrum-dependent systems from EW attack or to deny a target the benefit of their spectrum-dependent systems.[137] Common EW techniques include jamming spectrum-dependent systems; using EM energy to convey misleading information to spectrum-dependent weapons (known as "electronic deception"); and radiating electronic energy on friendly frequencies and

---

[128] *Id.*

[129] *Id.*

[130] Ian Bremmer, *The Technopolar Moment: How Digital Powers Will Reshape the Global Order*, FOREIGN AFFS. (Oct. 19, 2021), https://www.foreignaffairs.com/articles/world/2021-10-19/ian-bremmer-big-tech-global-order [https://perma.cc/FBK2-QC72].

[131] *See How Technology Builds Resilience in Critical Infrastructure Security*, N. CAROLINA CENTR. UNIV. (Apr. 19, 2022), https://online.nccu.edu/blog/technology-in-critical-infrastructure-security/ [https://perma.cc/5DAK-47YE].

[132] AIR FORCE DOCTRINE PUBLICATION 3–85, ELECTROMAGNETIC SPECTRUM OPERATIONS 1 (2023).

[133] DRAGAN POLJAK & MARIO CVETKOVIC, HUMAN INTERACTION WITH ELECTROMAGNETIC FIELDS 2 (1st ed. 2019).

[134] *Id.*

[135] *Id.*

[136] JOINT CHIEFS OF STAFF 3-13.1*,* ELECTRONIC WARFARE NO. G1-7 (2012).

[137] Air Force Doctrine Publication 3-85, *supra* note 132, at 4; *see also* Lorber, *supra* note 1, at 976–77.

electronic systems to act as an EW bulletproof vest, shielding them from EW attacks.[138]

EW and cyberwarfare exist in two very different domains, but they are comparable enough to justify a comparative LOAC analysis. Both seek to deny the enemy the benefit of their electronic devices. Both operate in an abstract domain, invisible to the human eye. And both use very similar strategies. Jamming and DDoS attacks both paralyze an electronic device by flooding it with signals. EW and cyberwarfare can cause a target to provide false data to its users.[139] In fact, the ongoing debate over Operation Orchard is whether EM deception or cyber deception is what misguided Syria's air defense system. Both uses of force are very difficult to definitively attribute to any attacker.[140] Both are low-cost, low-risk weapons compared to conventional arms.[141] Both are long-distance weapons that have no trouble crossing through borders and buildings.[142]

These EW and cyberwarfare comparisons have their limits, of course. A blast of EM energy can directly injure or kill a person in a kinetic attack, while cyberattacks are all non-kinetic and cannot directly cause injury or death.[143] A computer virus can infect computers and websites all over the world within minutes, while even the strongest EW attack can only affect the people and objects in a small area. The EW and cyberwarfare comparison is imperfect, but there is no perfect analogy.[144] Given the strong parallels between EW and cyberwarfare, the established

---

[138] JOINT CHIEFS OF STAFF 3-13.1, *supra* note 136, at 134.

[139] Thomas R. Burks, *Cyberspace, Electronic Warfare, and a Better Jus Ad Bellum Analogy*, 82 A.F. L. REV. 1, 6–8 (2022).

[140] Kristen E. Eichensehr, *The Law and Politics of Cyberattack Attribution*, 67 UCLA L. REV. 520, 522–23 (2022).

[141] CYBERPOWER AND NATIONAL SECURITY 423–24 (Franklin D. Kramer et al. eds., 2009); Burks, *supra* note 139, at 6–8.

[142] Burks, *supra* note 139, at 6–8.

[143] Joseph M. Nielsen, *Electromagnetic Conflict: The Implications of New Methods of Warfare and the Need For International Action*, 45 BROOKLYN J. INT'L L. 809, 812–13 (2020) ("Such [directed-energy] weapons have been modestly developed by states to be less lethal for use against humans in crowd-control type situations, a goal that can be achieved by scaling back the frequencies of the electromagnetic wave being emitted. When such electromagnetic energy is emitted against targets at noncontrolled levels, however, these waves can cause immeasurable damage to the brain and body. As stated by Dr. Elizabeth Plourde of EMF Freedom, '[w]e can liken this assault to being machine gunned. All of our cells are getting holes and leaking, our blood brain barrier is getting holes and leaking, and our gut is leaking.'").

[144] Burks, *supra* note 139, at 9–10.

rules and norms governing EW ought to inform the hotly contested role of cyberspace in international law.[145]

A. THE TYPES OF EW FORCE

Department of Defense policy recognizes three kinds of EW use of force, and this Article proposes applying that same standard to classifying cyberattacks.[146] The most peaceful use of force, Electronic Protection (EP), involves EW actions taken to protect personnel and property from harm.[147] EP examples include applying conductive coatings on EM devises to protect them from EM attacks, deploying reflective shields on military satellites to defect incoming laser beams, or monitoring the EMS in one's own airspace to detect potential threats.[148] None of these are hostile acts that damage other states or invade their sovereign territory, so, under *Nicaragua*'s use-of-force framework, EP's use of force does not rise to the level of armed force.

By stark contrast, Electronic Warfare Support (ES) involves the use of the EMS to harm people or property in support of a conventional armed attack.[149] Defensive ES activity includes firing an EM pulse at an incoming drone swarm to disable them, or using a radar station to jam an energy jammer and restore the station's ability to monitor the skies.[150] Offensive ES activity includes directed energy attacks, which can be lethal to people.[151] By harming another state's people or property, defensive and offensive ES alike meet *Nicaragua*'s definition of armed force. On a sufficient scale or gravity, such uses of armed force can constitute an armed attack.

For the third category of EW use of force, Electronic Attacks (EA) involve the use of the EMS to damage, neutralize, or destroy personnel, facilities, or equipment, but not in support of any conventional armed force.[152] Instead, these are standalone attacks. Like any other use of armed

---

[145] *Id.* ("Thus, that differences exist between two otherwise remarkably similar items is not necessarily the death of the analogy. This is particularly true when, as is the case here, the differences are what makes the analogy feasible.").

[146] JOINT CHIEFS OF STAFF 3-13.1, *supra* note 136, at I-6.

[147] *Id.*

[148] *Id.* at GL-7.

[149] *Id.*

[150] *Id.* at I-5.

[151] *Id.*

[152] *Id.* at I-4.

force, an EA of sufficient scale and gravity would constitute an armed attack. What would be sufficient? Scholars have offered no clear solution to that question, but even with that difference of opinion, the three categories still offer far more clarity to the current formlessness of cyberspace. Adopting these categories to cyberattacks would establish three kinds of cyber use of force: Self-Protective, Combat Support, and Standalone.

Self-Protective uses of cyberspace protect personnel, facilities, and equipment from harm.[153] Examples of this kind of use include creating strong passwords or firewalls that block unauthorized access to one's own websites, deploying antivirus and anti-malware software that detects and removes threats from one's cyberspace, or setting up honeypot websites that attract cyberattacks and provide the victim with a chance to study and reverse engineer the incoming cyberattacks. None of these are an aggressive or hostile use of cyberspace, so none of this activity could qualify as "armed force."

Combat Support lies at the other end of the spectrum of armed force as it involves the use of cyberspace to harm people or property in support of a conventional armed attack.[154] Defensive Combat Support causes harm in support of a conventional armed attack, but also in self-defense.[155] Examples include uploading spyware to monitor hostile actors, attacking a computer network in order to disable an ongoing cyberattack, or hacking into and disabling military satellites to disrupt a conventional military operation. For example, in 2016, US Cyber Command launched Operation Glowing Symphony, a campaign of cyberattacks targeting ISIS communication networks in an effort to slow its ability to plan and coordinate attacks and to stop its recruitment effort and propaganda dissemination.[156]

Offensive Combat Support describes cyberattacks that assist a conventional attack, and not in self-defense.[157] Operation Orchard fits squarely into this mold, if it used a cyberattack to disrupt Syrian air defenses and pave the way for an air strike. Similarly, DDoS attacks on Ukrainian banking and defense networks in 2022, along with the

---

[153] *Id.* at I-6.

[154] *Id.* at I-4.

[155] *Id.* at I-5-6.

[156] Joanna Jarose, *Reconsidering the Definition of 'Attack' and 'Damage' in Cyber Operations During Armed Conflict: Emerging Subsequent State Practice*, 44 ADELAIDE L. REV. 317, 318–19 (2023).

[157] JOINT CHIEFS OF STAFF 3-13.1, *supra* note 136, at I-6.

disruption of Ukraine's KA-SAT satellite network, paved the way for Russia's ground invasion of Ukraine. Because these cyberattacks harmed people and property and furthered an incoming or ongoing armed conflict, they should qualify as armed force. As such, any such cyberattack that rises to a sufficient scale or gravity should also constitute an armed attack. Such large-scale and grave uses of cyber force function no differently than an air campaign or artillery barrage that "softens" a target for an incoming attack.

This category of cyberattack is precisely where the effects-based, method-based, and target-based schools of thought break down. The use of cyberwarfare in Operation Orchard and in Russia's invasion of Ukraine did not harm any people or property; yet the effects of both attacks were indistinguishable from the effects of conventional uses of force. Similarly, the method-based calculation would dismiss each of these attacks for using unsophisticated, everyday cyberweapons instead of military-grade cyberweapons like the Stuxnet Virus. Only a target-based analysis would recognize the cyberattack on Syria's air defense system and Ukraine's military cyberspace as an armed use of force, since those are both military targets.

B. STANDALONE ATTACKS

For all the clarity that the three categories of force could bring into cyberspace, its third category for standalone attacks begs the question: in cases of standalone attacks, where should international law draw the line between cybercrime and cyberwarfare? Nearly all of the cyberattacks covered earlier in Part I (such as the Elk Cloner, SCA Virus, Morris Worm, and the Apple iCloud Hack) are mundane, everyday cyberattacks with no apparent connection to the world of armed conflict. Responding to such attacks with armed force is intuitively excessive, but the boundary between cybercrimes and cyberwarfare is not always as intuitively obvious.

For example, throughout 2012, an allegedly Iranian hacktivist group launched unusually sophisticated DDoS attacks on American financial institutions, in what they called Operation Ababil.[158] The US government responded with an aggressive cyber campaign of its own, taking down botnet command-and-control servers, in effect, tearing apart

---

[158] Annie Fixler, *The Cyber Threat from Iran after the Death of Soleimani*, 13 CTC SENTINEL 2 (2020).

the cyber infrastructure behind the DDoS attacks.[159] But, if the attacks simply resume from some other botnet servers, and American cybersecurity experts could pinpoint the source of these relentless attacks to a building in Tehran, would the US have lawful authority to treat this as an armed attack and then destroy that building in self-defense?

The law of EM attacks offers no promising solutions, since it is the source of this standalone attack vagueness. Possibly the most popular solution to the standalone EM attack issue is to draw the line at the reversibility of the attack.[160] This is a standard that avoids the issues of effects-based, target-based, and modality-based analyses by merging the key aspects of them all into a practical, more objective question: how long will it take for the victim to recover?[161]

For example, even in peacetime, authoritarian states often jam satellite transmissions to block politically or religiously inconvenient messaging from entering their state.[162] These jamming attacks inflict no damage.[163] Instead, they stop unwanted satellite transmissions into their territory.[164] This may be a nuisance to other states, as the jamming often interrupts satellite signals in general, including signals that reach many other states.[165] But, under this theory of non-kinetic armed conflict, such a standalone attack is not an act of war because it falls so low on the spectrum of reversible-irreversible attacks.

By contrast, hitting a satellite with strong EM signals would cause irreversible damage by frying the satellite's circuits or causing it to crash into a field of space debris. If this EM attack clearly comes from a state, then the attack would constitute a use of armed force. Pursuant to the umbrella of *jus in bello* rules and norms, the two states would automatically be in a state of armed conflict.[166]

The trouble with this popular model is its inclusivity. Inclusivity may be important in multicultural societies, but an overarching goal of LOAC is to avoid including peaceful noncombatants as lawful military

---

[159] AUSTEN GIVENS ET AL., *Forecasting Iranian Government Responses to Cyberattacks*, 13 J. ADVANCED MILITARY STUD. 1 (2022).

[160] Defabo, *supra* note 122, at 259–64.

[161] *Id.* As much as this sounds like effects-based reasoning, the fact is that it can take very little effort to recover from what is otherwise a very damaging attack on subject targets, while the slightest damage to other targets, in other scenarios, would be irrecoverably damaging.

[162] *Id.* at 254–59.

[163] *Id.*

[164] *Id.* at 274.

[165] *Id.*

[166] *Id.* at 259–64.

targets.[167] If a ninth-grade prankster in Pittsburgh tests out a homemade jammer that happens to send a military satellite crashing into a field of debris, should the irreversible damage of that incident really permit the victim state to call in an air strike? This reversible-irreversible model also assumes, without justification, that the EMS is so unique and incomparable to other weapons or domains as to require its own unique LOAC rules and norms. But, as something that can serve civilian or military purposes, the EMS is, by definition, a dual-use object; there is a well-established set of LOAC rules and norms that govern when the use of dual-use objects constitutes an armed attack.[168]

Instead of inventing a new, untested, and clunky model to categorize standalone attacks, international law can and should draw from its own pre-existing models—not only because the pre-existing models have had ample time to develop and address unexpected issues, but also because this issue with categorizing standalone attacks is, fundamentally, a question that has already been asked and answered.

In the recent wars in Iraq and Afghanistan, coalition forces faced a historically unprecedented number of civilians participating in combat against them.[169] Like standalone EM attacks, civilian participation in hostilities defies easy categorization. Like standalone EM attacks, civilian participation in hostilities in Iraq and Afghanistan was often sporadic, isolated, and not in support of any military campaign. They often lived as peaceful civilians, except for the brief moments when they were locked in violent combat with coalition forces.

As early as 2003, the International Committee of the Red Cross (ICRC) recognized the need to urgently clarify how LOAC should treat

---

[167] *Al Bahlul*, 820 F. Supp. at 1188.

[168] Dinstein, *supra* note 92 (analyzing dual-use objects under LOAC and explains how their military use can render them lawful targets).

[169] David Wallace et al., *Direct Participation in Hostilities in the Age of Cyber: Exploring the Fault Lines*, 12 HARV. NAT'L SEC. J. 164, 167 (2021) ("Civilians contribute to nearly every war effort, and always have. Throughout history, non-military personnel have supplied logistic, economic, administrative, and political support to parties in armed conflicts. . . More recently, however, belligerents have begun using civilians in capacities that involve greater or more direct participation in hostilities. Some commentators have referred to this phenomenon as the 'civilianization of armed conflict.' Prior studies have identified at least four developments that contribute to civilians' growing participation in hostilities: (1) the privatization of warfare, 3(2) a long-term shift toward non-international versus international armed conflicts, (3) the greater use of civilian proxies by States, and (4) the expanding role civilians play in high-technology warfare.").

standalone attacks from civilians.[170] Over the next six years, it consulted with forty to fifty legal experts from military, governmental, and academic backgrounds to create a set of rules that would strike the right balance.[171] The Geneva Conventions provide some foundation with the rule that combatants may only intentionally target lawful targets.[172] To do that, they must distinguish between lawful and unlawful targets.[173] Civilians are unlawful targets; they enjoy protection from intentional attack.[174] But, that protection is not absolute. Additional Protocol I to the Geneva Conventions suspends those protections "for such time as [civilians] take a direct part in hostilities."[175] In light of the wars in Iraq and Afghanistan, the ICRC sought to clarify two key questions about that framework: what acts constitute direct participation in hostilities (DPH), and how long does this DPH status last?

In 2009, the ICRC released its Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law.[176] The ICRC's guidance is that there are three "constitutive elements" of DPH: Threshold of Harm, Direct Causation, and Belligerent Nexus.[177] An act meets the threshold requirement if it is likely to harm the military operations or military capacity of a party to the armed conflict.[178] An act directly causes a result if there are few, if any, intervening causes between the act and the result.[179] And an act meets the belligerent nexus requirement if it is also specifically intended to directly cause the harm.[180]

---

[170] Michael N. Schmitt, *Deconstructing Direct Participation in Hostilities: The Constitutive Elements*, 42 INT'L L. & POL. 697, 709 (2010).

[171] Int'l Comm. of the Red Cross, Overview of the ICRC's Expert Process (2003–2008), https://www.icrc.org/en/doc/assets/files/other/overview-of-the-icrcs-expert-process-icrc.pdf [https://perma.cc/CKR2-BSXN].

[172] Gervais, *supra* note 20, at 71.

[173] *Id*. at 73.

[174] *Id.*

[175] Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), at art. 51, Dec. 7, 1979, 1125 UNTS 3; *see also* Jay C. Jackson, *Applying the U.S. and ICRC Standards for Direct Participation in Hostilities to Civilian Support of U.S. Military Operations*, 79 A.F. L. REV. 53 (2018).

[176] Schmitt, *supra* note 170, at 697–98.

[177] *Id.* at 698–99.

[178] *Id.* at 712–13; *see also* Wallace et al., *supra* note 169, at 179 (noting that the "array of qualifying harm is not limited to the infliction of death, injury, or destruction. . .", unlike the Tallinn Manual's effects-based proposal, which regards cyberattacks as armed force only if they result in such effects).

[179] Schmitt, *supra* note 170, at 726; *see also* Wallace et al., *supra* note 169, at 179.

[180] Schmitt, *supra* note 170, at 735; *see also* Wallace et al., *supra* note 169, at 180.

Under this framework, a civilian directly participates in hostilities if they are shooting at or kidnapping combatants; laying improvised explosive devices; equipping, instructing, or transporting military personnel; disseminating military intelligence; or preparing, transporting, or positioning weapons or military equipment.[181] This DPH guidance covers a wide variety of actions, while still protecting the many civilians who are only indirectly involved in armed conflict—for example, by providing finances, food, or shelter to armed forces.[182]

This same guidance clarifies when LOAC governs standalone cyberattacks. Under the ICRC's guidance, a standalone cyberattack constitutes direct participation in hostilities when it directly and intentionally harms the victim state's military capacity. In the same way that a civilian directly participates in hostilities by shooting at or kidnapping combatants, a standalone cyberattack directly participates in hostilities by launching DDoS attacks on military communications systems or weapons platforms. Similarly, the cyber equivalent of laying improvised explosive devices would be deploying malware in a manner intended to harm the victim state's military capacity. For other acts, comparisons are unnecessary. Gathering and disseminating military intelligence, for example, is an act of DPH, whether one does it with a set of binoculars and a radio or through cyber means, such as spyware.

The ICRC's framework is an imperfect analogy, since it presumes that the activity takes place during an ongoing armed conflict. Meanwhile, the defining feature of standalone attacks is that they do *not* take place during an ongoing armed conflict. Still, the ICRC's three-part framework is immensely useful to the extent that it defines what cyber actions should constitute an armed use of force. From there, LOAC doctrines would proceed as usual, by determining if the use of armed force constitutes an armed attack, if the armed conflict that the armed force creates constitutes an international or non-international armed conflict, and so forth.[183] This DPH-centered distinction between "armed" and "unarmed" standalone cyberattacks offers far more clarity than the current "I know it when I see it" approach.

---

[181] *See* Nila Melzer, *Interpretive Guidance on the Notion of Direct Participation in Hostilities Under International Humanitarian Law, Int'l Comm. of the Red Cross* (May 2009), https://www.icrc.org/en/publication/0990-interpretive-guidance-notion-direct-participation-hostilities-under-international [https://perma.cc/SE4V-JSYP].

[182] *Id.* at 52–53.

[183] *See Nicar. v. U.S.*, *supra* note 80, at ¶¶ 218-19.

The standalone cyberattacks covered in Part I help put this definition into practice. The 2012-era cyberattacks in Operation Ababil originated from Iran and targeted the US financial sector by striking the New York Stock Exchange and a number of banks, such as J.P. Morgan Chase and Bank of America.[184] Even after spending millions of dollars on cybersecurity improvements and countermeasures, the banks continued suffering disruptions from Operation Ababil's DDoS attacks.[185] Despite its Iranian origin and the possible involvement of the Iranian government, Operation Ababil supported no conventional military operation and did nothing to harm US military operations or military capacity. As such, even if cybersecurity personnel could pinpoint the source of the attack to a building in Tehran, the US president's range of lawful responses should not include, for example, cruise missiles. At its scale, Operation Ababil would be more comparable to a bank robbery than a military attack.[186]

By contrast, military force would be a lawful option if the attack set its sights on military targets instead, like the 2019 Hamas-led cyberattack explored in Part II, or if the attack caused more substantial harm to its civilian targets. For instance, the three weeks of significant disruptions that Estonia's finance, communications, and other sectors experienced in 2007 arguably qualify as an armed attack, as it directly and intentionally harmed Estonian military capacity. That 2007 attack approached the scale and gravity of a so-called "fire sale," a multi-stage, catastrophic cyberattack that brings down all, or at least much, of a state's critical infrastructure.[187] The plot of *Live Free or Die Hard* revolves around a cyberattack that shuts down transportation systems, financial systems, and utilities around the US.[188] The grounded flights, loss of

---

[184] Mathew J. Schwartz, *FBI Briefs Bank Executives on DDoS Attack Campaign*, DARK READING (May 14, 2013), https://www.darkreading.com/cyberattacks-data-breaches/fbi-briefs-bank-executives-on-ddos-attack-campaign [https://perma.cc/F5Y3-MM3R].

[185] *Id.*

[186] And contrary to the idea that bank robberies do not cost the taxpayers millions of dollars, a long list of bank robberies have stolen millions of dollars, and even hundreds of millions of dollars. *See The 10 Biggest Bank Robberies of All Time,* MONEYWISE (Aug. 5, 2022), https://moneywise.com/life/entertainment/the-biggest-bank-robberies-of-all-time [https://perma.cc/CL54-RKCC].

[187] Pablo Bermúdez, *Fire Sale Attack: The Greatest Threat Facing Peru in the 21st Century*, A-GLOSS (2021), https://aglossgroup.com/en/news/fire-sale-attack-the-greatest-threat-facing-peru-in-the-21st-century-pablo-bermudez/ [https://perma.cc/LVK3-F2JC] ("The Fire Sale is an all-out cyber warfare attack that performs a systematic three-stage attack on an entire nation's computing infrastructure. The hackers called it the Fire Sale because 'Everything must go' analogy to auctioning off products in a store that survived a fire.").

[188] *Live Free or Die Hard* (20th Century Fox 2007).

banking data, and widespread blackouts and water shortages from an attack of that scale could result in mass panic, looting, and uncontrollable lawlessness.[189]

As over-the-top as that seems, it is really more of an understatement. Just as a cyberattack on a Los Angeles hospital redirected emergency patients in an effort to kill them,[190] a large-scale cyberattack of that nature could target air traffic control systems and redirect planes into each other's airspace. Just as a 2021 hacking targeted a Florida water treatment plant in an effort to dangerously increase the level of lye in the water supply, a larger version of that attack could target chemical plants and oil refineries in an effort to cause explosions and toxic leaks.[191]

Just as a 2013 Iranian hacking group hacked into the Bowman Avenue Dam in New York, a successful hack into, or Stuxnet-like attack against, the Hoover Dam (Nevada), Oroville Dam (California), Grand Coulee Dam (Washington), Glen Canyon Dam (Arizona), or Fort Peck Dam (Montana) would devastate entire regions of the US.[192] There is also the "Skynet scenario," in which a hacker group or their artificial intelligence program gains unauthorized control over nuclear missiles and then sends those missiles on their merry way.[193] These are extreme and unlikely scenarios. But there are very skilled and highly motivated people trying to achieve those outcomes, and they may have the resources and support of a powerful government backing them up.[194]

---

[189] *Id.*

[190] *See* Greenberg, *supra* note 7.

[191] Jenni Bergal, *Florida Hack Exposes Danger to Water Systems*, STATELINE (Mar. 10, 2021), https://stateline.org/2021/03/10/florida-hack-exposes-danger-to-water-systems/ [https://perma.cc/KUT5-KTAZ].

[192] Press Release, Office of Public Affairs, Department of Justice, Seven Iranians Working for Islamic Revolutionary Guard Corps-Affiliated Entities Charged for Conducting Coordinated Campaign of Cyber Attacks Against U.S. Financial Sector (Mar. 24, 2016), https://www.justice.gov/opa/pr/seven-iranians-working-islamic-revolutionary-guard-corps-affiliated-entities-charged [https://perma.cc/9NTZ-KH3Q]; Carrieann Stocks, *Evolving Cybersecurity Threats to Hydropower Dams*, INT'L WATER POWER & DAM CONST. (June 12, 2024), https://www.waterpowermagazine.com/analysis/evolving-cybersecurity-threats-to-hydropower-dams/ [https://perma.cc/252R-9E2H].

[193] *Terminator 3: Rise of the Machines* (Warner Bros. Pictures 2003) (depicting an artificial intelligence program becoming self-aware, deciding that the human civilization is a threat to its survival, then taking control of the U.S. nuclear arsenal and launching nuclear missiles at Russia in order to trigger a nuclear war); Jarrod H. Stuard & James McGhee, Is Skynet the Answer? Rules for Autonomous Cyber Response, in EVOLUTION OF CYBER TECHNOLOGIES AND OPERATIONS TO 2035, ADVANCES IN INFO. SEC., (Cham Springer ed., 2015) (discussing the legal frameworks for autonomous cyber responses, and using Skynet as a reference point).

[194] Press Release, Office of Public Affairs, Department of Justice, Five Russian GRU Officers and One Civilian Charged for Conspiring to Hack Ukrainian Government (Sept. 5, 2024),

C. CRITIQUES

To be clear, this Article's proposal is only a start. Applying the three categories of EW to cyberattacks and the DPH test to standalone attacks would add badly needed clarity to this area of the law, but questions remain. For example, EP involves no harm, since it amounts to nothing more than shielding satellites from laser attacks or shielding electronics by adding protective coating. But the equivalent self-protective cyberspace actions, such as monitoring websites for malware, can easily become (or at least appear to become) a hostile act. A worm meant only to destroy a specific cyber threat could do so with unintentionally harmful effects, and it can unintentionally spread far beyond its intended targets. This is what happened when the Morris Worm caused unintentional damages, the Stuxnet worm spread far beyond Iran and infested two hundred thousand computers worldwide, and the Russian malware attack launched into Ukraine unintentionally spread worldwide, causing $10 billion in damages.[195] Cyberspace is called the "Inter*net*" and the "world wide *web*" for very good reason: it is a deeply interconnected system, with no borders, so any orders that a cyber program executes can cause effects far beyond what the programmers intended.

Similarly, in cyberspace, the difference between defensive and offensive actions might only become apparent in hindsight. For instance, when Hezbollah officials decided, in 2024, to use pagers and walkie-talkies instead of cell phones for operational security, they came across a website selling exactly what they needed, and at unbelievably good prices.[196] The prices were, in fact, too good to believe: the Israeli government had set up the website, and it was more than willing to ship to Hezbollah a slightly modified version of the sixteen thousand electronics

---

https://www.justice.gov/opa/pr/five-russian-gru-officers-and-one-civilian-charged-conspiring-hack-ukrainian-government [https://perma.cc/LRK5-2VC6].

[195] Michael Schmitt & Jeffrey Biller, *The NotPetya Cyber Operation as a Case Study of International Law, EJIL: Talk!*, BLOG EUROPEAN J. INT'L L. (July 11, 2017), https://www.ejiltalk.org/the-notpetya-cyber-operation-as-a-case-study-of-international-law/ [https://perma.cc/97DF-E9GW]; Wandulgi Lewis Kiiru, *Attribution and State Responsibility in Cyber Warfare: A Case Study of the NotPetya Attack* (Dec. 2019) (L.L.B. dissertation, Strathmore Law School) (on file with Strathmore Law School).

[196] Maya Gebeily, et al., *How Israel's Bulky Pager Fooled Hezbollah*, REUTERS (Oct. 15, 2024, 9:00 PM) https://www.reuters.com/graphics/ISRAEL-PALESTINIANS/HEZBOLLAH-PAGERS/mopawkkwjpa/ [https://perma.cc/4ZCJ-N5YR] (this website also came with online forums discussing the products).

that it purchased.[197] The cyber operation then morphed into an EM operation. After presumably using the devices to eavesdrop on Hezbollah operations and locate its secretive leadership, Israeli officials exploded the devices in September 2024, injuring three thousand Hezbollah operatives.[198] All of this began with just a website, passively occupying a little corner of cyberspace. Even with the benefit of hindsight, is it really an act of aggression to host a website with aggressively good prices?

Similarly, without the benefit of hindsight, it is often unclear if a cyberattack supports a conventional attack. Many cyberattacks support an incoming instead of ongoing armed attack, such as Russia's February 2022 cyberattack on Ukraine in the hours leading up to its invasion. Perhaps an armed attack will only proceed if the cyberattack achieves a devastating enough effect. Perhaps a cyberattack takes place during an armed conflict but has nothing to do with that conflict. In conflict zones, "ongoing armed conflict" is often a matter of perspective. For instance, did the Stuxnet attack take place during an ongoing armed conflict between Israel and Iran? Since 1979, relations between the two states have been poor, to put it lightly, but only in the last few months have their conventional armed forces traded blows. Do North Korean cyberattacks on South Korea take place during an ongoing armed conflict, or has the Korean armed conflict ended? There is no definitive answer. These are legal questions, but they may as well be philosophical questions instead.

Lastly, a defining feature of cyberattacks are their anonymity. Identifiable human beings are involved in physical attacks. Even for attacks carried out in the EMS, such attacks take place in a physical space and have a very limited range. By contrast, cyberattacks take place in a digital space that exists only in the minds of computers. These attacks can strike anywhere in the world, anytime; cyberspace knows no borders. Cyberattacks are carried out not by identifiable people but by software, executing a malicious code. A programmer may have an identifiable programming style, but the more identifiable it is, the easier it is for any other programmer to copy that style. Typically, if cybersecurity experts cannot identify an attacker's identity, they can only attribute an attack to an attacker based on the attack's site, size, and/or sophistication.[199]

---

[197] Reuters, *Pager Plot: How Massad Sold Explosive Devices to Hezbollah?*, THE EXPRESS TRIBUNE (Dec. 23, 2024), https://tribune.com.pk/story/2517847/pager-plot-how-mossad-sold-explosive-devices-to-hezbollah [https://perma.cc/7MEN-H7P2].

[198] *Id.*

[199] Heajune Lee, *Public Attribution in the U.S. Government: Implications for Diplomacy and Norms in Cyberspace*, 6 POL'Y DESIGN & PRAC. 198 (2023).

This attribution problem creates two issues, at least as far as this analysis is concerned. First, even if a cyberattack clearly justifies the use of military force in response, is it just as clear who or where the attacker is? As tragic as a cyberattack may be, it only adds to the tragedy if the retaliation harms people or property that have nothing to do with it.

Second, the more leeway that states receive to treat cyberattacks as armed attacks, the easier it becomes for bad actors to abuse their discretion. Cyberattacks take place in the shadows, so it is not difficult for states to claim that a vicious cyberattack has taken place and then do as they wish with their armed forces. States could as easily carry out a cyberattack on themselves, unleash their armed forces, and then conveniently bring the cyberattack to an end when the time is right. Cyberspace may offer the ideal option for states in search of a false flag attack operation.[200]

IV. CONCLUSION

Cyberspace blurs the once-clear distinctions between geopolitics, armed force, and crime. This blurring only intensifies as cyberattacks become an increasingly frequent part of major crimes and large-scale combat operations alike.[201] The EP/ES/EA categories and DPH test provide a clear framework for determining when a cyberattack, even a standalone one, involves the armed use of force and constitutes an armed attack. As such, applying these categories and tests to cyberattacks would reduce the ambiguity created by cyberspace.

This Article's hybrid test bridges the gap between the UN Charter's legal framework and the novel, recent developments that cyberspace operations created. The test also ensures that, even when a cyberattack crosses the line into an act of war, victim states must still keep their response measured, proportional to the threat, and rooted in LOAC

---

[200] Peter R. Mansoor, *False-Flag Operations*, HOOVER INST., Feb. 23, 2022 (overviewing the history of false flag operations, starting with ships at sea flying literal false flags in order to appear to belong to other states). While false flag attacks are closely associated with Nazi Germany (for the Reichstag Fire and the Gleiwitz Incident) and Russia (for the Mainila Shelling that preceded its invasion of Finland and the apartment bombings that preceded its Chechnya war), U.S. history has its share of false flag operations, such as The Gulf of Tonkin Incident and Operation Northwoods (a plan to stage attacks on U.S. assets to justify an invasion of Cuba, which President John F. Kennedy rejected); *see* CHARLES RIVER EDITORS, OPERATION NORTHWOODS: THE HISTORY OF THE CONTROVERSIAL GOVERNMENT PLAN TO STAGE FALSE FLAG ATTACKS ON AMERICANS AND BLAME CUBA (2022).

[201] Lorber, *supra* note 1, at 965–69.

principles. Where the target-based, method-based, and effects-based tests all ignore context and fail to tackle the nuanced reality of cyberattacks, this hybrid test offers a rigorous and flexible method to navigate the otherwise murky distinction between cybercrime and cyberwarfare.

Instead of completely overhauling LOAC or singling out cyberspace for a different set of LOAC rules, the hybrid test proposed in this Article draws from LOAC's established rules and norms and merely applies them to the digital battlefield. Instead of contradicting or ignoring these principles, it reconciles them with the realities of this digital battlefield. As that digital battlefield continues swelling, in both breadth and depth, the urgency of addressing it and bringing it within LOAC framework grows.

Until that happens, the unclear role of cyberspace in international law creates a dangerous, destabilizing vacuum in foreign affairs. Individuals, armed groups, and states will continue exploiting that vacuum and ambiguity to full effect, at low cost and almost no risk to themselves, but at the cost of billions of dollars to regular US citizens, the US government, and US companies of all sizes. Of all the threats to US national security, few are as persistent, pervasive, and costly as cyberattacks. In fact, cyberattacks cost the US far more than any other country,[202] and the most damaging, far-reaching hacks into American infrastructure took place in 2024.[203] The US, and the international community as a whole, cannot afford to let cyberspace remain a lawless frontier.

---

[202] Steve Morgan, *Cybercrime to Cost the World $10.5 Trillion Annually by 2025*, CYBERCRIME MAG. (Nov. 13, 2020), https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/ [https://perma.cc/7JBW-TJDY].

[203] *See, e.g.*, Ana Swanson & David E. Sanger, *China Hacked Treasury Dept. in 'Major' Breach, U.S. Says*, N.Y. TIMES (Dec. 30, 2024), https://www.nytimes.com/2024/12/30/us/politics/china-hack-treasury.html [https://perma.cc/9PEE-928Z].