UC Irvine Law Review

Volume 10 | Issue 4 Article 6

6-2020

Privatized Cybersecurity Law

Ido Kilovaty

Privatized Cybersecurity Law

Ido Kilovaty*

Tech companies have gradually and informally assumed the role of international lawmakers on global cybersecurity issues. But while it might seem as if the international community and Internet users are the direct beneficiaries of private tech industries' involvement in making law, there are many questions about this endeavor that require a thorough examination. The end goal and risks associated with such ventures are largely obscure and unexplored.

This Article provides an analysis of how tech companies are effectively becoming regulators on global cybersecurity, based on states' inability to overcome geopolitical divides on how cyberspace ought to be regulated globally. This Article looks primarily at three separate proposals representing the larger trend of the privatization of cybersecurity law: the Digital Geneva Convention, the Cyber Red Cross, and the Cybersecurity Tech Accord. These, as well as other initiatives, reflect the gradual and uncontested assimilation of private tech companies into the machinery of international lawmaking.

This Article argues that state governments, civil society organizations, Internet users, and other stakeholders need to step back and carefully evaluate the dangers of ceding too much lawmaking control and authority to the private tech sector. These private actors, while not yet on an equal footing to states, are increasingly displacing states as they seek to create their own privatized and unaccountable version of cybersecurity law.

* Frederic Dorwart and Zedalis Family Fund Assistant Professor of Law, University of Tulsa, College of Law; Cybersecurity Policy Fellow, New America; Visiting Faculty Fellow, Center for Global Legal Challenges, Yale Law School; Affiliated Fellow, Information Society Project, Yale Law School. The author wishes to thank the fellows of the Information Society Project at Yale Law School, Oona Hathaway, Claudia Haupt, Tiffany Li, Mason Marks, Frank Pasquale, Bob Spoo, and Ari Ezra Waldman for their feedback and the editors at UC Irvine Law Review for their extraordinary editorial work.

INTRODUCTION

The global regulation of cybersecurity is one of the most contentious topics on the international legal plane.[1] States, which are perceived as the most suitable entities to regulate cyberspace globally, are largely incapable of reaching a consensus on what such law would look like due to their geopolitical differences.[2] In this

1. David P. Fidler, *The UN Secretary-General's Call for Regulating Cyberwar Raises More Questions than Answers*, COUNCIL ON FOREIGN REL. (Mar. 15, 2018), https://www.cfr.org/blog/un-secretary-generals-call-regulating-cyberwar-raises-more-questions-answers [https://perma.cc/63XS-429C] ("How these [international law] rules apply in cyberspace has been extensively discussed across the UN and elsewhere for many years, often with controversy overshadowing consensus.").

2. JACK GOLDSMITH, CYBERSECURITY TREATIES: A SKEPTICAL VIEW 4 (2011) ("For most cybersecurity issues, it is not clear that a mutually beneficial deal is possible in theory . . . . [T]here are

structural and normative vacuum, tech companies are seizing the opportunity to create norms and rules for cyber operations, essentially creating a privatized version of cybersecurity law.[3]

This "governmentalization" of private tech companies is occurring in many contexts that were previously government-regulated.[4] For example, many tech companies have recently begun to perform a quasi-judicial function within their platforms.[5] Amazon is but one example of a company where judicial functions are privatized through the widely used dispute resolution system between vendors and consumers.[6] Facebook's "Supreme Court" is another instance of a tech company deciding to make certain quasi-judicial determinations on content moderation, reflecting the overall trend of governmentalization in tech.[7]

Tech companies' desire for power through governmentalization is also currently reshaping the international legal regulation of cybersecurity. By international legal regulation of cybersecurity, I mean the international law applicable to cyberspace, as the "fifth domain" of warfare,[8] where state governments and non-state actors are acting in offense and defense, and civilians are victimized by cyber operations. In this domain, Microsoft is leading the charge in creating norms that would govern the law applicable to global cybersecurity,[9] a

---

deep and fundamental clashes not only over what practices should be outlawed but also and more broadly over what the problem is."); Rebecca Crootof, *International Cybertorts: Expanding State Accountability in Cyberspace*, 103 CORNELL L. REV. 565, 640–41 (2018) ("For a variety of reasons, however, a constitutive cybersecurity treaty may not be possible, especially if it attempts to regulate state conduct. At the most basic level, there are few cyber-related subjects that permit mutually beneficial deals for states with differing technological capabilities, differing vulnerabilities, and differing beliefs about the appropriate amount of governmental control over the internet or the dangers posed by free speech. Indeed, not only do states desire to regulate different activities in cyberspace, many states see others' proposed norms as being antithetical to their own concerns.").

3. *See* Shin-yi Peng, *"Private" Cybersecurity Standards? Cyberspace Governance, Multistakeholderism, and the (Ir)relevance of the TBT Regime*, 51 CORNELL INT'L L.J. 445, 450 (2018) (arguing that "privatization of governance" is a result of "governments' lack of requisite technical expertise and the flexibility to deal with ever-more complex regulatory tasks").

4. *See* Janosik Herder, *The Power of Platforms*, PUB. SEMINAR (Jan. 25, 2019), https://publicseminar.org/essays/the-power-of-platforms/ [https://perma.cc/5HT6-NGAB].

5. Frank Pasquale, *Digital Capitalism—How to Tame the Platform Juggernauts*, WISO DIREKT (June 2018), http://library.fes.de/pdf-files/wiso/14444.pdf [https://perma.cc/49DG-TWE3]; *see also* Kate Klonick, *The New Governors: The People, Rules, and Processes Governing Online Speech*, 131 HARV. L. REV. 1598, 1617 (2018).

6. Pasquale, *supra* note 5, at 2–3; Jane K. Winn, *The Secession of the Successful: The Rise of Amazon as Private Global Consumer Protection Regulator*, 58 ARIZ. L. REV. 193, 201–03 (2016) (explaining how platforms, Amazon in particular, are governors with respect to dispute resolution between consumers and vendors).

7. Kate Klonick & Thomas Kadri, *How to Make Facebook's Supreme Court Work*, N.Y. TIMES (Nov. 17, 2018), https://www.nytimes.com/2018/11/17/opinion/facebook-supreme-court-speech.html [https://perma.cc/F7VP-CPKT].

8. *War in the Fifth Domain*, ECONOMIST (July 1, 2010), https://www.economist.com/briefing/2010/07/01/war-in-the-fifth-domain [https://perma.cc/C67T-W3JM].

9. Brad Smith, *The Need for a Digital Geneva Convention*, MICROSOFT (Feb. 14, 2017), https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/ [https://perma.cc/9NN6-7SGM]. For a summary of how Microsoft's endeavors fit in with in the broader

phenomenon some refer to as norm entrepreneurship.[10] These norms are the binding directives that seek to protect Internet users from state-sponsored cyberattacks and strengthen their cybersecurity protection.[11]

There are many good reasons for Microsoft to take the lead in developing such norms. The primary explanation is that Internet users are vulnerable, and their vulnerability, particularly to state-sponsored activity online, negatively impacts the reputation of and trust in the tech industry.[12] After all, Internet users in such cases could see their personal information compromised,[13] access to banking and emergency services curtailed,[14] or devices such as vehicles,[15] pacemakers,[16] webcams,[17] and insulin pumps hacked.[18] These are all real and documented

---

picture of private-sector cyber norms, see ANGELA MCKAY ET AL., MICROSOFT, INTERNATIONAL CYBERSECURITY NORMS: REDUCING CONFLICT IN AN INTERNET-DEPENDENT WORLD (2014), http://aka.ms/cybernorms [https://perma.cc/4R6E-RBPA]; Garrett Hinck, *Private-Sector Initiatives for Cyber Norms: A Summary*, LAWFARE (June 25, 2018), https://www.lawfareblog.com/private-sector-initiatives-cyber-norms-summary [https://perma.cc/P83B-H65M].

10. Tim Maurer, *Private Companies Take the Lead on Cyber Security*, WAR ON THE ROCKS (May 4, 2018), https://warontherocks.com/2018/05/private-companies-take-the-lead-on-cyber-security/ [https://perma.cc/5S3F-BKCF]; *see also* Martha Finnemore & Duncan B. Hollis, *Norms for Global Cybersecurity*, 110 AM. J. INT'L L. 425, 447 (2016) ("Norm entrepreneurs are critical to norm emergence not only because they call attention to an issue but because they frame it—they use language that names, interprets, and dramatizes the problem—and on that basis propose a norm to address it.").

11. Brad Smith, *34 Companies Stand Up for Cybersecurity with Tech Accord*, MICROSOFT (Apr. 17, 2018), https://blogs.microsoft.com/on-the-issues/2018/04/17/34-companies-stand-up-for-cybersecurity-with-a-tech-accord/ [https://perma.cc/FP8T-98PJ] (introducing the four governing principles of the Cybersecurity Tech Accord).

12. Kristen E. Eichensehr, *Public-Private Cybersecurity*, 95 TEX. L. REV. 467, 502–03 (2017) (listing the incentives for the tech industry to pursue public-private partnerships in global cybersecurity, including that "the public-relations benefits of some of the actions are substantial," for example, "attributing cyber intrusions to state-sponsored attackers is excellent advertising").

13. Jeff Kosseff, *Defining Cybersecurity Law*, 103 IOWA L. REV. 985, 987 (2018) ("A day rarely passes without another report of a major cybersecurity incident. Hackers routinely breach the systems of retailers, stealing consumer credit card data, social security numbers, and other valuable personal information.").

14. Joshua Davis, *Hackers Take Down the Most Wired Country in Europe*, WIRED (Aug. 21, 2007, 12:00 PM), https://www.wired.com/2007/08/ff-estonia/ [https://perma.cc/RKZ9-DHGZ] (describing cyber-attacks on Estonia in 2007 that disabled access to banking, emergency, and government services).

15. Andy Greenberg, *Hackers Remotely Kill a Jeep on the Highway—With Me in It*, WIRED (July 21, 2015, 6:00 AM), https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/ [https://perma.cc/4FHN-HDKK].

16. Lily Hay Newman, *A New Pacemaker Hack Puts Malware Directly on the Device*, WIRED (Aug. 9, 2018, 12:30 PM), https://www.wired.com/story/pacemaker-hack-malware-black-hat/ [https://perma.cc/EA5Q-NJEV].

17. Lorenzo Franceschi-Bicchierai, *How 1.5 Million Connected Cameras Were Hijacked to Make an Unprecedented Botnet*, VICE: MOTHERBOARD (Sept. 29, 2016, 9:03 AM), https://www.vice.com/en_us/article/8q8dab/15-million-connected-cameras-ddos-botnet-brian-krebs [https://perma.cc/BE7R-P5WD].

18. Jim Finkle, *J&J Warns Diabetic Patients: Insulin Pump Vulnerable to Hacking*, REUTERS (Oct. 4, 2016, 4:05 AM), https://www.reuters.com/article/us-johnson-johnson-cyber-insulin-pumps-e/jj-warns-diabetic-patients-insulin-pump-vulnerable-to-hacking-idUSKCN12411L [https://perma.cc/5HCU-GEFA].

consequences of malicious cyberspace activity. With these potentially devastating consequences in mind, it is understandable why the next logical step would be to develop binding norms and rules to effectively deter such activity.[19]

But there is a caveat, which is that private tech companies are de facto becoming the legislators of global cybersecurity law, with no guarantee of respect for values such as accountability,[20] transparency, or fairness.[21] And while the norms proposed by these companies may sound innocuous[22]—involving terms such as "peace,"[23] "humanitarian,"[24] and "Red Cross"[25]—a closer look reveals their potential difficulties.

This Article argues that private tech companies are effectively becoming legislators of global cybersecurity law, with strings attached. This argument is grounded in the premise that states have failed to respond to this normative vacuum and are currently unable to do so.[26] Accordingly, as Julie Cohen has recently argued, "dominant platforms' role in the international legal order increasingly resembles that of sovereign states."[27] Tech companies' increasing involvement in the international legal system is challenging its structure, values, and future.

Some would contest the premise that states are unable or unwilling to regulate global cybersecurity. They claim that the international legal order, through long-standing principles and frameworks, already provides civilians a variety of

---

19. Joseph Nye, *Deterrence and Dissuasion in Cyberspace*, 41 INT'L SECURITY 44, 60 (2017) ("A fourth mechanism by which dissuasion works is norms and taboos. Normative considerations can deter actions by imposing reputational costs that can damage an actor's soft power beyond the value gained from a given attack.").

20. Laura A. Dickinson, *Privatization and Accountability*, 7 ANN. REV. L. SOC. SCI. 101, 117 (2011) ("Privatization has become a dominant reality of twenty-first-century governance. Accordingly, scholars and policymakers will need to seek new ways to embed core principles of accountability into this emerging form of state power.").

21. Eichensehr, *supra* note 12 (providing an in-depth analysis of the public law values implicated by public-private partnerships in cybersecurity).

22. Julie E. Cohen, *Law for the Platform Economy*, 51 U.C. DAVIS L. REV. 133, 201 (2017) (arguing that platforms who self-identify as "conscientious, neutral stewards of the global digital infrastructure, set a lofty tone that elevates the more self-interested processes of strategic positioning operating continually in the background").

23. *Demand Digital Peace Now*, MICROSOFT, https://digitalpeace.microsoft.com/ [https://perma.cc/B588-TME6].

24. Brad Smith, *We Need to Modernize International Agreements to Create a Safer Digital World*, MICROSOFT (Nov. 10, 2017), https://blogs.microsoft.com/on-the-issues/2017/11/10/need-modernize-international-agreements-create-safer-digital-world/ [https://perma.cc/CYB9-Z6GN].

25. Smith, *supra* note 9.

26. *See, e.g.*, Michael Schmitt & Liis Vihul, *International Cyber Law Politicized: The UN GGE's Failure to Advance Cyber Norms*, JUST SECURITY (June 30, 2017), https://www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms/ [https://perma.cc/5VCG-6F92].

27. Cohen, *supra* note 22, at 199–203 (providing various examples of platforms independently engaging in institutional and legal reform, and observing that "the role of platforms in the emergent global legal order is doubly under construction").

protections from state-sponsored cyberattacks.[28] Indeed, international law does protect civilians from government overreach in assorted ways under the auspices of international human rights law.[29] These include their rights to life,[30] due process,[31] privacy,[32] assembly,[33] speech,[34] access to information,[35] and even basic access to the Internet itself.[36] Directing state-sponsored cyberattacks at civilians, depending on their effects, could potentially be in violation of these human rights obligations.[37] Additionally, once an armed conflict emerges, international humanitarian law offers its own set of protections with the aim of reducing the suffering and adverse consequences that are so endemic to war.[38] For example, international humanitarian law prohibits the direct targeting of civilians by warring parties.[39] Today, this reflects

---

28. Harold Hongju Koh, *International Law in Cyberspace*, 54 HARV. J. INT'L L. ONLINE 1, 3 (2012) ("Yes, international law principles do apply in cyberspace. . . . [N]o. Cyberspace is not a 'law-free' zone where anyone can conduct hostile activities without rules or restraint.").

29. Gabor Rona & Lauren Aarons, *State Responsibility to Respect, Protect, and Fulfill Human Rights Obligations in Cyberspace*, J. NAT'L SECURITY L. & POL'Y 503, 505 (2016) ("At the emergence of international human rights, it was anticipated that its principles would extend to all media, regardless of new technological advancements.").

30. International Covenant on Civil and Political Rights art. 6(1), Dec. 16, 1966, S. TREATY DOC. NO. 95-20, 999 U.N.T.S. 171, 174–75 [hereinafter ICCPR]; G.A. Res. 217 (III) A, Universal Declaration of Human Rights, at art. 3 (Dec. 10, 1948) [hereinafter UDHR].

31. ICCPR, *supra* note 30, at art. 9, 999 U.N.T.S. at 175–76; UDHR, *supra* note 30, at art. 10.

32. ICCPR, *supra* note 30, at art. 17(1), 999 U.N.T.S. at 177–78; UDHR, *supra* note 30, at art. 12.

33. ICCPR, *supra* note 30, at art. 21, 999 U.N.T.S. at 178; UDHR, *supra* note 30, at art. 20(1).

34. ICCPR, *supra* note 30, at art. 19(2), 999 U.N.T.S. at 178; UDHR, *supra* note 30, at art. 19.

35. ICCPR, *supra* note 30, at art. 19(2), 999 U.N.T.S. at 178; UDHR, *supra* note 30, at art. 19.

36. Human Rights Council Res. 32/13, U.N. Doc. A/HRC/32/L.20 (June 27, 2016); David Kravets, *U.N. Report Declares Internet Access a Human Right*, WIRED (June 3, 2011, 2:47 PM), https://www.wired.com/2011/06/internet-a-human-right/ [https://perma.cc/22CA-JK89] ("The Special Rapporteur calls upon all states to ensure that Internet access is maintained at all times, including during times of political unrest. In particular, the Special Rapporteur urges States to repeal or amend existing intellectual copyright laws which permit users to be disconnected from Internet access, and to refrain from adopting such laws.").

37. Some, however, would argue that the application of international human rights law to a cyberattack against civilians originating from abroad is not as straightforward. *See* Cordula Droege, *Get Off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians*, 94 INT'L REV. RED CROSS 533, 547 (2012) ("[I]nternational human rights law might apply, but would a computer network attack, conducted from the other side of the globe against civilian infrastructure, fulfil the requirement of effective control for the purpose of applicability of human rights law? Also, to what extent would human rights law provide sufficient protection against the disruption of infrastructure the effects of which on the lives of civilians is not necessarily immediately identifiable?").

38. Hans-Peter Gasser, *International Humanitarian Law and the Protection of War Victims*, INT'L COMMITTEE RED CROSS (Nov. 30, 1998), https://www.icrc.org/en/doc/resources/documents/misc/57jm93.htm [https://perma.cc/V3VX-ELXJ] ("[I]nternational rules which limit the effects of war on people and property, and which protect certain particularly vulnerable groups of persons. That is the goal of international humanitarian law, with the Geneva Conventions and their Additional Protocols as its main expression and an important body of customary law as a decisive supplementary source of law.").

39. *Rule 1. The Principle of Distinction Between Civilians and Combatants*, INT'L COMMITTEE RED CROSS, https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1_rul_rule1 [https://perma.cc/6V8Z-ZGMN] ("The parties to the conflict must at all times distinguish between civilians and

indisputable and binding customary international law.[40] By analogy, civilians ought to be protected from direct cyberattacks, as they are not directly involved in the conflict and therefore are not legitimate military objectives.[41] Similarly, the same body of law restricts indirect harm to civilians by limiting the amount of permissible collateral damage involving civilians and their property.[42] It may therefore appear as if, at least in theory, there is sufficient law applicable to state-sponsored cyberattacks.[43]

While these assessments appear straightforward and backed by long-standing practice,[44] emerging state activity—and most importantly the tech industry's activity in cyberspace—makes these case-by-case assessments far more complicated than they may seem at first blush.[45] Some questions that remain unresolved are: What does it mean to *directly target* a civilian using malware that is inherently indirect?[46] Does such targeting need to be lethal? Or would directly disabling civilian computer systems and networks also constitute a violation of that rule? Does collateral damage only mean deaths and injuries to civilians? Or does it include other harms, such as data loss, denial of service, manipulation, spread of fear and terror, and major inconvenience?[47] Would election interference be in violation of international human

---

combatants. Attacks may only be directed against combatants. Attacks must not be directed against civilians.").

40. *Id.* ("State practice establishes this rule as a norm of customary international law applicable in both international and non-international armed conflicts.").

41. 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(2), *opened for signature* Dec. 12, 1977, 1125 U.N.T.S. 3, 26 [hereinafter Protocol I] ("The civilian population as such, as well as individual civilians, shall not be the object of attack. Acts or threats of violence the primary purpose of which is to spread terror among the civilian population are prohibited.").

42. *Id.* art. 51(5)(b), 1125 U.N.T.S. at 26 ("[A]n attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated.").

43. *See generally* Oona A. Hathaway et al., *The Law of Cyber-Attack*, 100 CALIF. L. REV. 817 (2012) (detailing the various international law rules applicable to cyberattacks).

44. Gary Brown & Keira Poellet, *The Customary International Law of Cyberspace*, STRATEGIC STUD. Q., Fall 2012, at 127 ("There is a body of customary law reflecting the extensive and virtually uniform conduct of nation-states during traditional warfare that is widely accepted and well understood—the law of war. Unfortunately, the application of the law of war to cyberspace is problematic because the actions and effects available to nations and nonstate actors in cyberspace do not necessarily match up neatly with the principles governing armed conflict.").

45. Michael N. Schmitt, *Grey Zones in the International Law of Cyberspace*, 42 YALE J. INT'L L. ONLINE 1 (2017) (identifying specific gaps in international law as it applies to cyberattacks).

46. Michael Gervais, *Cyber Attacks and the Laws of War*, 30 BERKELEY J. INT'L L. 525, 567–68 (2012) ("However, there are cyber attacks that deliberately target objects to kill civilians or destroy civilian objects. Such attacks are clearly unlawful under the law of armed conflict. In practice, however, cyber attacks targeting civilians have been more of an inconvenience than a threat to life or safety.").

47. Ido Kilovaty, *Virtual Violence—Disruptive Cyberspace Operations as "Attacks" under International Humanitarian Law*, 23 MICH. TELECOMM. & TECH. L. REV. 113, 137–39 (2016) ("The primary shortcoming of a narrow reading of collateral damage is that the most severe disruptive cyber operations would be far more humanitarianly dangerous than physical destroying a house belonging to a civilian. That is to say, that disruption effects can be far more serious than physical ones. In that sense, reconsidering the scope of collateral damage is essential.").

rights law?[48] Or would dated conceptions of sovereignty and prohibited intervention limit such a determination? International law seems unable to answer these with a reasonable degree of specificity.

These questions are far from theoretical. In fact, they represent a significant gap in international law that is not easily solvable. This indeterminacy poses a serious and immediate danger to civilians who find themselves in the midst of a cyber conflict. Tech companies that promote "norms," "rules," and "principles" for global cybersecurity realize that this point in time is an opportunity for them to seize the role of international lawmakers.[49] Clearly, private entities have no authority to create "law" as that term is typically understood within the U.S. constitutional system. But internationally, tech companies may be able to create certain prescriptions that will affect state practice and eventually permeate legal systems, becoming authoritative without being grounded in the democratic legitimacy, public interest, or accountability expected from "real" legislators.[50] This is largely enabled through customary international law—states' repeated practices that create a sense of binding legal obligation.[51]

This represents a departure from the state-centric approach of creating international law, a phenomenon which this Article calls the privatization of

48. Jens David Ohlin, *Did Russian Cyber Interference in the 2016 Election Violate International Law?*, 95 TEX. L. REV. 1579, 1583 (2017) ("[I]t would seem as if Russia's cyber intrusion violated the human rights of the owners of the various e-mail accounts, including John Podesta and several DNC officials.").

49. Maurer, *supra* note 10 ("[I]t is only the latest sign that what norms govern cyber space and the global governance of cyber security—or, rather, the lack thereof—have captured the attention of corporate boardrooms around the world.").

50. The term "real legislators" is somewhat elusive in the international legal context. Many have argued that non-state actors may be influencing international law in a variety of ways, a so-called "bottom-up" approach. *See* Jon P. Jurich, *Cyberwar and Customary International Law: The Potential of a "Bottom-up" Approach to an International Law of Information Operations*, 9 CHI. J. INT'L L. 275 (2008); Janet Koven Levit, *A Bottom-Up Approach to International Lawmaking: The Tale of Three Trade Finance Instruments*, 30 YALE J. INT'L L. 125 (2005); Michael N. Schmitt & Sean Watts, *Beyond State-Centrism: International Law and Non-State Actors in Cyberspace*, 21 J. CONF. & SECURITY L. 595 (2017). In the privacy law context, see Ari Ezra Waldman, *Privacy Law's False Promise,* 97 Wash. U. L. Rev. 773, 790–92 (2020) (describing the process of legal endogeneity—how privacy law is understood by corporations as a matter of compliance rather than a set of substantive privacy protections).

51. *Customary International Law*, LEGAL INFORMATION INSTITUTE: WEX, https://www.law.cornell.edu/wex/customary_international_law [https://perma.cc/ZE3T-RHNL] (last visited Dec. 14, 2019) ("Customary international law refers to international obligations arising from established international practices, as opposed to obligations arising from formal written conventions and treaties. Customary international law results from a general and consistent practice of states that they follow from a sense of legal obligation.").

cybersecurity law.[52] This Article explores this new phenomenon[53] while describing the trends that are currently reshaping the international legal order on cybersecurity. The primary purpose of this Article is to identify potential structural and normative difficulties arising from the tech industry's growing involvement in international lawmaking. These difficulties should encourage states, civil society, and the public to step back and reexamine the privatization of cybersecurity law. Part I introduces the narrative of the emerging privatization of cybersecurity law led by the tech industry. Part II delves into how this phenomenon challenges and disrupts the international legal order, potentially heralding an important transformation of the basic tenets of international law. Part III explores the concrete ways in which the privatization of cybersecurity law is undermining norms and values such as democracy, transparency, accountability, and neutrality. In closing, I conclude with a call for caution with respect to the increasing regulatory role of private tech companies and a reconsideration of international law's effort to regulate cybersecurity globally.

I. PRIVATIZED CYBERSECURITY LAW

Privatized cybersecurity law is the emerging phenomenon of tech companies creating rules, norms, and principles for conduct in cyberspace, primarily the conduct of states vis-à-vis other states and individual users.[54] Private tech companies, for many reasons that this Article will cover, hold the view that it is their duty to protect civilians in cyberspace, whether proactively from state-sponsored cyberattacks or passively by enhancing civilian infrastructure security.[55] While

52. "Privatization" in that context does not necessarily pass any moral judgement on platforms' endeavors to create global cybersecurity law. While this Article is generally critical of these steps, there are many other contexts where privatization of cybersecurity may actually be beneficial. *See, e.g.*, Nathan Alexander Sales, *Privatizing Cybersecurity*, 65 UCLA L. REV. 620, 687–88 (2018) (looking at various market-based solutions to incentivize black-hat and gray-hat hackers to sell their vulnerabilities on the white-hat market; the author, while recognizing the benefits of the private sector in promoting cybersecurity, is nonetheless cautious, arguing "[t]here's no question that the government has a critical role to play—indeed, the leading role—in securing cyberspace, whether through traditional means like law enforcement or through less conventional regulatory approaches").

53. In contrast, non-state actors have already been involved in influencing the outcomes of political and diplomatic negotiations. *See* Alex Grigsby, *The End of Cyber Norms*, 59 GLOBAL POL. & STRATEGY 109, 109 (2017) ("Think tanks, foundations and some technology companies joined in as norm entrepreneurs, hoping to make their mark on diplomatic negotiations."). However, the phenomenon introduced by this Article—lawmaking by digital platforms—is different.

54. *See A Digital Geneva Convention to Protect Cyberspace*, MICROSOFT, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW67QH [https://perma.cc/8WAW-CC9P].

55. Among the Cybersecurity Tech Accord's commitments is one to "protect all of our users and customers everywhere," which focuses on active protection "from cyberattacks—whether an individual, organization or government—irrespective of their technical acumen, culture or location, or the motives of the attacker, whether criminal or geopolitical" and a more passive protection where companies promise that they "will design, develop, and deliver products and services that prioritize security, privacy, integrity and reliability, and in turn reduce the likelihood, frequency, exploitability, and severity of vulnerabilities." *Id.*

seemingly innocuous, this involves a considerable acquisition of prescriptive power by tech companies, which this Part analyzes and reviews.

In 2017, Brad Smith, President and Chief Legal Officer of Microsoft, gave a provocative speech at the United Nations in Geneva, Switzerland.[56] Smith's talk started with an overview of the creation of the International Committee of the Red Cross (ICRC), the world's most central and active humanitarian institution. Henry Dunant, a Swiss businessman, established the ICRC in 1863 after witnessing the horrors of war at the Battle of Solferino in June 1859, when thousands of soldiers lost their lives or were severely injured.[57] While the atrocities of war were undoubtedly Dunant's motivation in convincing governments to support the creation of the ICRC, according to Smith, it was also the new technologies of warfare that led Dunant and others to rethink the limits and the humanitarian aspects of waging war between nations.[58] These new technologies directly caused massive atrocities, suffering, and casualties that convinced Dunant that an international humanitarian organization was urgently needed.[59]

Smith argued that we are at a similar moment in history, where cyberspace is the catalyst for a new arms race.[60] That arms race is leading to the creation of cyber weapons in an almost legally and ethically unrestricted manner, which leaves civilians vulnerable to severe harm and suffering. Smith, therefore, is of the view that he is in a similar position as Dunant, in that the tech industry, witnessing the horrors of global cyberattacks, should create its own version of an ICRC for cyberspace—a Cyber Red Cross (CRC) of sorts. While Smith's motivations may be genuine, this view represents a significant shift in the tech industry's view of its own role in society.

To demonstrate the humanitarian harms of cyberattacks, Smith provided the recent example of the WannaCry ransomware.[61] In May 2017, the malware WannaCry affected as many as 200,000 computers in 150 nations around the

---

56. *Brad Smith Takes His Call for a Digital Geneva Convention to the United Nations*, MICROSOFT (Nov. 9, 2017) [hereinafter *Brad Smith Takes His Call*], https://blogs.microsoft.com/on-the-issues/2017/11/09/brad-smith-takes-call-digital-geneva-convention-united-nations/ [https://perma.cc/5634-5JU2].

57. *Henry Dunant (1828–1910)*, INT'L COMMITTEE RED CROSS (Apr. 6, 1998), https://www.icrc.org/en/doc/resources/documents/misc/57jnvq.htm [https://perma.cc/X9LR-X85S].

58. *Brad Smith Takes His Call*, *supra* note 56.

59. Brad Smith & Carol Ann Browne, *What's to Be Learned from the Founding of the Red Cross?*, MICROSOFT, https://blogs.microsoft.com/today-in-tech/whats-to-be-learned-from-the-founding-of-the-red-cross/ [https://perma.cc/K5AV-YDJW] ("Across Europe a consensus quickly emerged that these technological advances for warfare required new humanitarian and organizational innovations in response.").

60. Steve Ranger, *Why Microsoft Is Fighting to Stop a Cyber World War*, ZDNET (Dec. 12, 2018), https://www.zdnet.com/article/why-microsoft-is-fighting-to-stop-a-cyber-world-war/ [https://perma.cc/NAL5-EZB5] ("Smith drew a parallel between the run-up to the First World War and the burgeoning cyberwar arms race today.").

61. Nicole Perlroth & David E. Sanger, *Hackers Hit Dozens of Countries Exploiting Stolen N.S.A. Tool*, N.Y. TIMES (May 12, 2017), https://www.nytimes.com/2017/05/12/world/europe/uk-national-health-service-cyberattack.html?module=inline [https://perma.cc/P996-U7UE].

world.[62] This was not a military-to-military kind of cyberattack, but rather an indiscriminate ransomware worm that infected any computer it touched.[63] Most notably, as many as 70,000 computers belonging to the United Kingdom's National Health Service hospital network were severely affected.[64] Smith's concerns, shared with many others around the world, are that cyberattacks on civilian infrastructure could result in significant humanitarian consequences, and that the law is largely silent on the matter.

Skeptics would argue that it was computers, not people, that were targeted and affected by the WannaCry ransomware. Therefore, what exactly is the *humanitarian* concern? This view could not be further from the truth. The adverse effects on medical computers and devices affected 7,000 patients scheduled to receive medical treatment on the day of WannaCry's mayhem.[65] Because computers have created mediated environments in which humans need computers to literally sustain life, attacks against computers will have clear and direct effects on human lives and well-being.[66] Cyberattacks, therefore, may have serious consequences for civilians, who rely on governments, businesses, critical infrastructure, transport, energy, and other individuals who themselves rely on the integrity and availability of computer systems and networks.[67]

Microsoft and many other tech companies clearly have a stake in promoting "peace" in cyberspace.[68] No business would want the government to use its infrastructure to engage in cyber conflict, especially if such engagement did not directly benefit their revenue, could negatively affect user trust, and was not

---

62. Elizabeth Piper, *Cyber Attack Hits 200,000 in at Least 150 Countries: Europol*, REUTERS (May 14, 2017, 3:23 AM), https://www.reuters.com/article/us-cyber-attack-europol/cyber-attack-hits-200000-in-at-least-150-countries-europol-idUSKCN18A0FX [https://perma.cc/8THY-TSJ3].

63. Press Briefing, The White House, Press Briefing on the Attribution of the WannaCry Malware Attack to North Korea (Dec. 19, 2017), https://www.whitehouse.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917/ [https://perma.cc/V4TL-6KBF] ("In May of this year, a dangerous cyberattack known as WannaCry spread rapidly and indiscriminately across the world.").

64. Sarah Neville, *NHS Systems to Be Strengthened After Cyber Attack*, FIN. TIMES (July 12, 2017), https://www.ft.com/content/ced6dd82-6709-11e7-9a66-93fb352ba1fe [https://perma.cc/YY6P-YGMV].

65. David Benady, *Cybersecurity: Have Lessons Been Learned Since the WannaCry Attack?*, GUARDIAN (Nov. 29, 2018), https://www.theguardian.com/delivering-digital-transformation/2018/nov/29/cybersecurity-have-lessons-been-learned-since-the-wannacry-attack [https://perma.cc/YEW6-YWQ6] ("Over a third of trusts and nearly 600 doctors' surgeries were hit by the virus, resulting in almost 7,000 patient appointments being cancelled.").

66. Tyler Elliot Bettilyon, *Cybersecurity Is About Much More than Hacking*, MEDIUM (Nov. 21, 2018), https://medium.com/s/story/cybersecurity-isnt-just-about-hacks-f11c7ad07660 [https://perma.cc/X45F-CAES] ("Digital systems now play a crucial role in banking, payroll, distribution chains, voting, social interaction, medicine, cars, planes, trains, implanted medical devices, and so on. Each and every one of these digital systems is a potential vulnerability.").

67. *Id.*

68. Ed Targett, *Microsoft Demands "Digital Peace"—What Does It Really Want?*, COMPUTER BUS. REV. (Oct. 1, 2018), https://www.cbronline.com/news/digital-peace-microsoft [https://perma.cc/N8JE-AVAH].

imposed coercively by regulators.[69] And even if it did benefit the tech company's profits, users' trust would be severely impacted.[70] Users are unlikely to approve of becoming pawns in conflicts between states, particularly if such conflicts are mediated by private tech companies. Tech companies themselves certainly do not want to perpetuate such a reality. Smith made this clear in his speech by highlighting how cyber warfare between nations is in fact an attack on civilians. He said,

> When there are attacks on cyberspace, they in fact are attacks on private property—it may be against the phone that is in your pocket, or the laptop that is on your desk, or the servers that are in our datacenter, or the cables that are underneath the ocean, that we operate, that connect datacenters together.[71]

The concerns put forward by Smith illustrate the reason why many tech companies believe that their duty to their users involves strengthening their products' cybersecurity—whether devices, software, or any other service on which civilians rely. By doing so, companies may make it harder for malicious actors to attack civilians, directly or indirectly, or at least increase the costs of such attacks to the point where malicious actors would become disincentivized from attacking civilians.[72] Tech companies not only passively protect their users by repelling malware and patching their products, but are also currently using the law and courts to proactively defend them by going after malicious actors before users are massively victimized by cyberattacks.[73] This is an example of the fairly well-established idea of a public-private partnership on certain national security and

---

69. Kristen E. Eichensehr, *Digital Switzerlands*, 167 U. PA. L. REV. 665, 691 (2019) ("One possible explanation for the companies' behavior is economic: the companies may assess that the posture of neutrality will best maximize their growth and profits going forward by increasing their appeal to users worldwide.").

70. *See id.* at 668, 683 ("They have global *users*, not just customers or shareholders . . . . [These] users rely on the company for services and trust the company to keep potentially sensitive information secure . . . . Unlike companies that merely sell goods to customers, the tech companies' relationship to their users is more intimate, more expansive, and more constant than even a series of recurring transactions.").

71. *Brad Smith Takes His Call*, *supra* note 56.

72. Daniel J. Solove, *Cybersecurity: Leviathan vs. Low-Hanging Fruit*, TEACH PRIVACY (June 24, 2015), https://teachprivacy.com/cybersecurity-leviathan-vs-low-hanging-fruit [https://perma.cc/B8ZF-AMMD] ("There are certainly many hackers with sophisticated technical skills and potent malicious technologies. These threats can seem akin to Leviathan—all powerful and insurmountable. It can be easy to get caught up focusing on the Leviathan and miss the low-hanging fruit of cybersecurity. This low-hanging fruit consists of rather simple and easy-to-fix vulnerabilities and bad practices. Cybersecurity is a garden of mostly low-hanging fruit. Pluck the fruit, and huge headway can be made in protecting data.").

73. Microsoft helps law enforcement authorities take down harmful botnets. *See, e.g.*, *Microsoft Teams Up with Law Enforcement and Other Partners to Disrupt Gamarue (Andromeda)*, MICROSOFT (Dec. 4, 2017), https://www.microsoft.com/security/blog/2017/12/04/microsoft-teams-up-with-law-enforcement-and-other-partners-to-disrupt-gamarue-andromeda/ [https://perma.cc/DL8F-DNFM] ("Today, with help from Microsoft security researchers, law enforcement agencies around the globe, in cooperation with Microsoft Digital Crimes Unit (DCU), announced the disruption of Gamarue, a widely distributed malware that has been used in networks of infected computers collectively called the Andromeda botnet.").

law enforcement issues.[74] Smith, and surely other tech industry leaders, believe it is their responsibility to take these steps to protect their users.

There may be another explanation for tech companies' nascent role as legislators of global cybersecurity law: the desire for power. The current state of affairs in global cybersecurity law allows tech companies to perform such a role, since states are entirely unable to maintain their inherent authority in collectively regulating global cybersecurity, for reasons discussed below. But first, to fully understand how tech companies may become such legislators, it is important to review the current "legislative" steps that Microsoft and other companies have engaged in.

A. Geneva 5.0

The world needs a Digital Geneva Convention, says Brad Smith.[75] There are simply too many cyberattacks targeting the private sector, and we need some kind of international legal framework that will commit actors to norms on cyberspace conduct.[76]

The idea that the world needs a fifth Geneva Convention[77] —a Geneva 5.0—to address humanitarian concerns in cyberspace and protect civilians from cyberattacks during peacetime is somewhat misguided. After all, the Geneva Convention's primary purpose is not only to protect civilians, but also to strike an acceptable balance between military necessity and humanitarian values.[78] As such, international humanitarian law authorizes the use of direct force against combatants and allows for collateral damage involving civilians and civilian property resulting from an attack, so long as that collateral damage is proportionate to the military advantage sought.[79] This is a problematic vision from the humanitarian perspective, since it still confers a rather broad degree of discretion on warring states. In peacetime, the protection of civilians is the *raison d'être* of international

74. Madeline Carr, *Public-Private Partnership in National Cyber-Security Strategies*, 92 INT'L AFF. 43 (2016).

75. Smith, *supra* note 9.

76. *Id.*

77. The four current Geneva Conventions focus on (1) wounded and sick soldiers on land during war; (2) wounded, sick, and shipwrecked military personnel at sea during war; (3) rights of and obligations in respect to prisoners of war; and (4) protection of civilians, including in occupied territory. *See The Geneva Conventions of 1949 and their Additional Protocols*, INT'L COMMITTEE RED CROSS (Oct. 29, 2010), https://www.icrc.org/en/doc/war-and-law/treaties-customary-law/geneva-conventions/overview-geneva-conventions.htm [https://perma.cc/UP2T-GXVQ].

78. Paul Weidenbaum, *Necessity in International Law*, 24 TRANSACTIONS GROTIUS SOC'Y 105, 110 (1938) ("The Conventions expressly declare to strike a balance between military necessity and a humane conception of warfare.").

79. *Rule 14. Proportionality in Attack*, INT'L COMMITTEE RED CROSS, https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1_rul_rule14 [https://perma.cc/93F9-4RJ7] ("Launching an attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated, is prohibited.").

human rights law, which seeks to protect civilians from governmental overreach.[80] The same protections ought to apply online.[81] Extending the rules and norms of wartime international humanitarian law to the peacetime use of cyberattacks is a dangerous move.[82] It would mean that some peacetime cyberattacks, when directed at military objectives, would be legal. It would also harm civilians in "indirect" ways, which international humanitarian law largely tolerates.

However, the idea the we may need a new Digital Geneva Convention generates some important and difficult questions with regard to the protection of civilians in cyberspace during armed conflict.[83] First and foremost, what is it about international humanitarian law at present that renders it ineffectual? Specifically, why is it that the tech industry, with Microsoft in the lead, decided that this ought to be their newest conquest?

As alluded to earlier, there are simply too many questions on how this law applies in different situations in cyberspace. One could argue that there are certain gaps in the law that leave civilians vulnerable to certain kinds of cyberattacks that produce negative effects for individuals and society at large.[84] The reason for that could be that either custom involving international humanitarian law or its accepted interpretation has not yet caught up with emerging offensive uses of cyberspace in

---

80. In the cybersecurity context, the question would be whether a foreign government mounting a cyberattack against another nation would satisfy the effective control standard required by international human rights law to determine its obligations vis-à-vis a foreign government's citizens. *See* Oona Hathaway et al., *Human Rights Abroad: When Do Human Rights Treaty Obligations Apply Extraterritorially?*, 43 ARIZ. ST. L.J. 389, 395 (2011) ("Nearly every other foreign and international body examined here concludes that countries that exert 'effective control' over a territory, person, or situation must observe basic human rights obligations.").

81. H.R.C. Res. 32/13, *supra* note 36, ¶ 1 ("[T]he same rights that people have offline must also be protected online.").

82. Francesca Casalini & Stefania Di Stefano, *State Behaviour in Cyberspace: Moving Away from a Military Discourse*, DIPLO (Mar. 15, 2018), https://www.diplomacy.edu/blog/state-behaviour-cyberspace-moving-away-military-discourse [https://perma.cc/5YS5-EY8S] ("Since it remains unclear when a cyber-operation attains the level of armed attack for the purposes of IHL, and since the aims pursued by Microsoft's proposal are largely different from those pursued by the laws of war, it would seem more appropriate to re-think the Microsoft proposal as an instrument that would seek to establish a system of Internet governance, and that does not aim at affecting or replacing any other existing legal regime. It could simply represent the acknowledgment that there are new phenomena that are in need of regulation. In this sense, the 'peacetime' qualification does not add value, and generates a risk that the proposed rules would be considered displaceable in times of war, whereas the particular relationship that exists between the state and the private sector in the cyber realm would persist even during an armed conflict. For these reasons, we suggest removing the peacetime qualification altogether.").

83. Tarah Wheeler, *In Cyberwar, There Are No Rules*, FOREIGN POL'Y (Sept. 12, 2018), https://foreignpolicy.com/2018/09/12/in-cyberwar-there-are-no-rules-cybersecurity-war-defense/ [https://perma.cc/P4JM-VURL] (providing an account of how the lack of rules may evolve into a full-scale cyberwar).

84. Paul Nicholas, *Filling the Gaps in International Law Is Essential to Making Cyberspace a Safer Place*, MICROSOFT (Mar. 27, 2018), https://www.microsoft.com/security/blog/2018/03/27/filling-the-gaps-in-international-law-is-essential-to-making-cyberspace-a-safer-place/ [https://perma.cc/UH92-9SE3].

armed conflict, which could result in lethal and nonlethal but dangerous harms.[85] As a result, there may be some considerable definitional and normative gaps that need to be addressed if we wish to maintain an adequate level of protection for civilians. For example, for an action to be an "attack," must it cause death, or would any other effects qualify?[86] Is civilian data an "object" protected from direct "attack"? How are nonlethal effects calculated in comparison to lethal effects in cyberspace?

Second, extending the law governing *war* to *peacetime* seems directly antithetical. That law, after all, is more permissive when it comes to civilian casualties and damage to their property, as wars often involve a certain degree of suffering or, in legalese, proportionate collateral civilian damage that is permissible under international humanitarian law.[87] Why does Geneva 5.0 make this dangerous leap? A simple explanation would be that this is a common conflation between *humanitarian* and *human rights* law, both striking their own balances and pursuing different values and policy goals. While human rights law has a role to play in both *peacetime* and *wartime*,[88] humanitarian law only applies in an armed conflict.[89]

But there may be a more complicated and less intuitive explanation, which stems from the nature of cyberattacks. That explanation has to do with the ever-blurring dividing line between war and peace.[90] The argument goes that international humanitarian law applies only during armed conflict.[91] Over the decades, however, conflicts have become more complex, involving non-state actors such as terrorist organizations and private militias. Some weapons, such as

85. Kristen E. Eichensehr, *Cyberwar & International Law Step Zero*, 50 TEX. INT'L L.J. 355, 374 (2015) ("[C]yber weapons create the possibility of actions that cause severe harm to the victim, but nevertheless do not result in physical damage or injury to persons. The paradigmatic example is an attack that wipes out information stored on a system or network, such as a stock exchange.").

86. Kilovaty, *supra* note 47, at 127 ("The key to incorporate disruptive cyber operations within the scope of 'attack' under IHL is to interpret 'acts of violence' as including cyber operations with disruptive effects."); *cf.* Pete Pascucci & Kurt Sanger, *Why a Broad Definition of "Violence" in Cyber Conflict Is Unwise and Legally Unsound*, JUST SECURITY (Mar. 8, 2017), https://www.justsecurity.org/38536/broad-definition-violence-cyber-conflict-unwise-legally-unsound/ [https://perma.cc/WH2L-BK78].

87. Stephen Petkis, *Rethinking Proportionality in the Cyber Context*, 47 GEO. J. INT'L L. 1431, 1440 (2016) ("According to this *jus in bello* conception of proportionality, a state must balance the 'concrete and direct' military advantage it is likely to obtain against any incidental harm its actions are likely to cause civilians.").

88. Oona Hathaway et al., *Which Law Governs During Armed Conflict? The Relationship Between International Humanitarian Law and Human Rights Law*, 96 MINN. L. REV. 1883 (2012) (offering three models to explain the role and applicability of international human rights law in armed conflict).

89. *Id.* at 1888 ("Humanitarian law applies only in situations of armed conflict; hence the applicability of this body of law turns on whether an armed conflict or occupation exists.").

90. *See, e.g.*, ROSA BROOKS, HOW EVERYTHING BECAME WAR AND THE MILITARY BECAME EVERYTHING: TALES FROM THE PENTAGON (2016); Rosa Brooks, *There's No Such Thing as Peacetime*, FOREIGN POL'Y (Mar. 13, 2015, 5:47 PM), https://foreignpolicy.com/2015/03/13/theres-no-such-thing-as-peacetime-forever-war-terror-civil-liberties/ [https://perma.cc/7WQ2-RBTK].

91. *See* Hathaway et al., *supra* note 88, at 1888.

cyberattacks, have become "democratized"[92] (accessible to non-state actors) and wield more disruptive than destructive power (though they can certainly be destructive). Therefore, their effects are not reaching the level of intensity usually associated with a traditional armed conflict, but it does not entirely feel like peacetime either.[93] It is an intermediate category, somewhere in between the two extremes of war and peace, that the law has failed to recognize and regulate.[94]

Rosa Brooks has long argued that we are overly obsessed with antiquated distinctions between wartime and peacetime.[95] This is a critical conversation to have with regard to cyber weapons, as they can cause massive disruption, potentially leading to humanitarian crises, but are rarely directly lethal. This is where the comfortable analogy between cyber and non-cyber weapons is not as obvious.[96] This leads to a seemingly simple question, though the answer may not be easy at all: What would be considered "cyber peace" and at what point does the use of cyber weapons reach the threshold of "cyber war"? How do we distinguish the regulation of cyber war from regular war, and is such a distinction even required? The question is further exacerbated by Microsoft's recent petition on "Digital Peace," in which "digital citizens" are demanding digital peace.[97] What does that mean, and who gets to answer that question?[98]

Third, it is important to acknowledge the identity and interests guiding the actors engaged in privatizing cybersecurity law. After all, international humanitarian

92. Grigsby, *supra* note 53, at 109 ("The online world is one of strategic instability, given the relative ease and stealth of state-sponsored attacks, and the fact that it is almost impossible to tell whether a purely defensive cyber action is in fact hostile.").

93. Michael Schmitt, *Five Myths in the Debate About Cyber War*, JUST SECURITY (Sept. 23, 2013), https://www.justsecurity.org/918/myths-debate-cyber-war/ [https://perma.cc/6CL9-Q5BW] (explaining that a non-international armed conflict involving only cyberattack would have two features: "First, the intensity criterion would require protracted cyberattacks causing extensive physical damage or death. Second, the organization criterion would generally exclude operations, no matter how severe, conducted by groups organized entirely online").

94. Alexander Greenawalt, *If War Is Everywhere, Then Must the Law Be Nowhere?*, 32 TEMP. INT'L & COMP. L.J. 25 (2018) (explaining that the distinction between war and peace is essential for determining whether killing is justified or not).

95. Rosa Brooks, *War Everywhere: Rights, National Security Law, and the Law of Armed Conflict in the Age of Terror*, 153 U. PA. L. REV. 675, 677 (2004) ("These binary distinctions [between war and peace] are no longer tenable. In almost every sphere, globalization has complicated once straightforward legal categories, but this is nowhere more apparent and more troubling than in the realms of armed conflict and national security law. Although the boundaries between 'war' and 'nonwar,' and between 'national security' and 'domestic issues,' have been eroding for some time, September 11 and its aftermath have highlighted the increasing incoherence and irrelevance of these traditional legal categories.").

96. Eichensehr, *supra* note 85, at 374.

97. *Demand Digital Peace Now*, *supra* note 23.

98. As one commentator observed: "The DGC [Digital Geneva Convention] picks and chooses International Humanitarian Law principles and taglines at its convenience, without fully developing the concepts." Raquel Vázquez Llorente, *A Digital Geneva Convention? The Role of the Private Sector in Cybersecurity*, LSE IDEAS STRATEGIC UPDATE, May 2018, at 10, http://www.lse.ac.uk/ideas/Assets/Documents/updates/LSE-IDEAS-The-Role-of-the-Private-Sector-in-Cybersecurity.pdf [https://perma.cc/MSU4-3VFA].

law was created by states and, mostly, for the benefit of states.[99] Why did the tech industry suddenly decide to take up the reins of protecting civilians in cyberspace? This desire for power in a space plagued with normative ambiguities may lead to some serious issues with respect to the absence of certain values such as transparency and accountability.

In many instances, these tech companies advocate for forming the aforementioned CRC, or "Cyber-ICRC."[100] But whereas the ICRC is a neutral organization that is not motivated by profits or capitalist power and is governed by clear rules, norms, and values, with the consent of state parties to the Geneva Conventions, that is not necessarily the case for the CRC. The CRC would involve tech companies in an unprecedented fashion, further enhancing their power and standing in the global community. From a normative-content perspective, Geneva 5.0 is far from the only prescription promoted by tech companies. The Cybersecurity Tech Accord, a set of rules that seventy global tech companies committed themselves to, is perhaps the most significant development with respect to the privatization of cybersecurity law.[101]

B. The Cybersecurity Tech Accord

To strengthen their commitment to their users, a group of global tech companies has signed the Cybersecurity Tech Accord, a public commitment to "protect and empower our users and customers, and thereby to improve the security, stability, and resilience of cyberspace."[102] Microsoft initiated this process in the spring of 2018, with over sixty global tech companies signing on the Accord's principles.[103] Underlying this Accord is the understanding that cyberspace has become the cornerstone of global society. Global society relies on the Internet for communication, business, entertainment, infrastructure, education, and much more. But such reliance creates fertile ground for criminal and state-sponsored offensive activity, which undermines the availability, confidentiality, and integrity of the data, services, and applications used throughout cyberspace.[104]

---

99. Eichensehr, *supra* note 85, at 366 ("[I]nternational law has traditionally operated at the level of sovereign States, and the independence of sovereigns engendered a strong tradition that States are bound only by international law to which they consent.").

100. Elaine Korzak & Herb Lin, *Proposal for a Cyber-International Committee of the Red Cross*, LAWFARE (Oct. 17, 2018, 8:25 AM), https://www.lawfareblog.com/proposal-cyber-international-committee-red-cross [https://perma.cc/B6H8-FHUT].

101. *A Digital Geneva Convention to Protect Cyberspace*, *supra* note 54.

102. *Id.*

103. Rob Wright, *Cybersecurity Tech Accord Expands with New Members, Partners*, TECHTARGET (Sept. 25, 2018), https://searchsecurity.techtarget.com/news/252449304/Cybersecurity-Tech-Accord-expands-with-new-members-partners [https://perma.cc/2UHE-8RNX] ("The Cybersecurity Tech Accord was first unveiled by Microsoft's president, Brad Smith, during his keynote at RSA Conference 2018.").

104. Isabella Uria, *Hacking the Election Conference (Write Up)*, YALE L. SCH. (Sept. 20, 2016), https://law.yale.edu/sites/default/files/area/center/isp/documents/hacking_the_election_conference_report_11.01.16.pdf [https://perma.cc/JSG7-CWMR] (quoting Professor Jack Goldsmith

The Cybersecurity Tech Accord contains merely four principles.[105] First, tech companies pledge to protect their users from cyberattacks by providing products and services with built-in security and privacy.[106] Second, tech companies will not provide assistance to governments or any other organization in the launch of cyberattacks.[107] Third, tech companies will educate users on tools available to them, and will support civil society, governmental, and organizational efforts in advancing global cybersecurity.[108] And, fourth, tech companies will create formal and informal partnerships to enhance cybersecurity—sharing information on threats, patching vulnerabilities, and encouraging global information-sharing to protect civilians and help in recovery efforts from cyberattacks.[109]

It would make sense for major tech companies to commit to these principles. Aside from being a positive public relations step, it is also a reliable and practical commitment, since these tech companies happen to control significant portions of the infrastructure, products, and services that populate cyberspace. Therefore, they believe that they ought to be the "first responders" in cyberspace.[110] These principles thus appear at first glance to be a positive development in protecting civilians from harmful cyber activity. But that value judgement only holds if we detach these principles from the tech economy and its motivations, which raises a variety of as-yet unanswered questions.[111] For example, what is the role of tech companies in enforcing and interpreting these principles?

C. A Cyber Red Cross

The idea of creating an organization whose expertise it is to resolve humanitarian crises in cyberspace has been promoted by several scholars for years.[112] Duncan Hollis and Tim Maurer, following a series of serious cybersecurity incidents, including against Sony, Target, Home Depot, and J.P. Morgan Chase, argued in 2015 that "the time is ripe for a bolder approach to cybersecurity . . . cyberspace could use a global cyber federation, a federation of non-governmental

---

as observing that "'the United States has the most robust cyber capability in the world, but it is also the most vulnerable,' due to its extensive dependence on computer systems in the public, private, and military sectors").

105. *A Digital Geneva Convention to Protect Cyberspace*, *supra* note 54.

106. *Id.*

107. *Id.*

108. *Id.*

109. *Id.*

110. *See* Lousie Hurel & Luisa Lobato, *Unpacking Cyber Norms: Private Companies as Norm Entrepreneurs*, 3 J. CYBER POL'Y 61, 63 (2018).

111. Andrew Keane Woods, *Tech Firms Are Not Sovereigns*, *in* HOOVER INST. AEGIS PAPER SERIES 3 (Sept. 27, 2018), https://www.hoover.org/sites/default/files/research/docs/woods_webreadypdf.pdf [https://perma.cc/4548-C744] (answering the question of what tech companies are up to: "making money").

112. Duncan Hollis & Tim Maurer, *A Red Cross for Cyberspace*, TIME (Feb. 18, 2015, 10:04 AM), https://time.com/3713226/red-cross-cyberspace/ [https://perma.cc/GBW9-9Y8F].

institutions similar to the role of the Red Cross . . . ."[113] Hollis and Maurer's vision is to make Computer Emergency Response Teams (CERTs) throughout the world the building blocks of this new "independent, neutral, and impartial" institution.[114] Their proposal involves neither for-profit private actors or state actors within the structure of this new institution.

It took three years for that proposal to be reexamined and reintroduced in a modified form. Herb Lin and Elaine Korzak have advocated for the creation of a "Cyber-International Committee of the Red Cross."[115] Lin and Korzak's reexamination was triggered by the creation of the Cybersecurity Tech Accord, discussed above. They believe its principles will only be effectuated if there is an institution to back them up.

The CyberPeace Institute, established in late 2019, is an example of such emerging CRC organization.[116] The CyberPeace Institute involves both for-profit and non-profit entities within an organization that seeks to protect civilians from cyber-attacks, assist in accountability, and advance international law norms for responsible behavior in cyberspace.[117] While it is too early to pass judgement on the CyberPeace Institute's mandate, there are some challenging issues that may require further attention in the years to come.

Some of these issues include whether the CyberPeace Institute will commit to principles of transparency, independence from corporate capture, neutrality vis-à-vis state governments, and accountability. While the CyberPeace Institute claims to be guided by these principles, it remains to be seen whether they can be upheld in practice. Of particular challenge are scenarios where: (1) certain tech corporations make profit off data collected and analyzed by the CyberPeace Institute; (2) the victim of a cyber-attack requesting assistance is a politically controversial organization (terrorist group, for example), forcing the Institute to decide whether to offer assistance or not; (3) there is a conflict between international law and norms created and practiced by the Institute; (4) there is a conflict between the mandate of existing institutions (ICRC, for example) and the Institute.

In the years to come, the CyberPeace Institute (and any other CRC) may face pushback from governments. For example, some governments may be concerned that their views are not fairly represented, that the investigative powers and expertise of the Institute may somehow prejudice their national security, or that their ability to create norms for cyberspace is preempted by the Institute's mandate. As always, some of these objections may be more reasonable than others.

These challenges notwithstanding, the idea of a CRC as a global institution seeking to promote stability and trust in cyberspace appears desirable. At the same

113. *Id.*

114. *Id.*

115. Korzak & Lin, *supra* note 100.

116. *See* CyberPeace Institute, *About Us*, https://cyberpeaceinstitute.org/about-us [https://perma.cc/K6PH-A9Y8] (last visited May 26, 2020).

117. *Id.*

time, it requires further unpacking. The debate on whether the world needs a CRC could be a debate over whether there is a need for: (1) a humanitarian assistance organization; (2) an independent institution for the investigation and attribution of cyberattacks; (3) a reliable cybersecurity expertise institution; (4) an institution creating and promoting norms for an ever-evolving cyberspace threat landscape; or (5) a neutral and apolitical institution performing an entirely professional function for global cybersecurity. More than anything, if tech companies become involved in a CRC scheme, it would essentially mean that they will possess insurmountable and unprecedented power in global cybersecurity governance. To illustrate that, I discuss these five concepts in turn.

1. Humanitarian Assistance

Say there is a cyberattack against critical infrastructure targets, such as the power grid, the Internet's backbone, or the healthcare sector, causing a serious humanitarian crisis. Which global institution has the capacity to effectively address such a crisis? The immediate association that comes to mind is the ICRC. The ICRC has indeed been at the forefront of humanitarian assistance, alleviating suffering, mitigating atrocities, and assisting in holding accountable those responsible. Indeed, the ICRC might be helpful for responding to some aspects of cyber-humanitarian crises. But could the ICRC assist in restoring affected computer systems and networks? Could it provide assistance to ensure that such a humanitarian disaster does not reoccur?

The CRC, therefore, would be the ICRC equivalent for humanitarian crises in cyberspace. It would assist in restoring affected targets, advise on best measures, and fill the gap where states are unwilling or unable to assist their own victimized subjects. This notion of humanitarian assistance is closely related to other functions often mentioned with regard to a CRC. For example, it could assist in investigation and attribution where victims cannot get their state's government to do so, whether because the state does not have the capacity or is unwilling. As Lin and Korzak argue, the CRC will "fill an assistance gap that is particularly felt by victims who lack the capacity or resources to respond to or recover from cyberattacks."[118]

2. Investigation and Attribution

Attribution, "the ability to confidently say who did it: which country, government agency, group, or even individual is responsible for a cyber intrusion or attack"[119] is key in assigning international responsibility. But because attackers

118. *Id.*

119. John Carlin, *Detect, Disrupt, Deter: A Whole-of-Government Approach to National Security Cyber Threats*, 7 HARV. NAT'L SECURITY J. 391, 396 (2016).

may leverage and benefit from anonymity,[120] attribution is often seen as one of the major challenges of global cybersecurity.[121]

Investigation and attribution—done neutrally, independently, professionally, and promptly—are critical functions in cyberspace that are currently institutionally absent from the structure of the global community.[122] Currently, if an entity (other than the government itself) becomes the victim of a cyberattack, that victim can only ask for assistance from its local law enforcement or, more broadly, the state. However, decisions on whether to investigate, how to proceed with an investigation, and who the culprit is are often affected by a series of political and strategic interests.[123] For example, will the victim's state blame a powerful nation for initiating a cyberattack if there are major economic interests involved with that nation? Should the state reveal its evidence at the expense of compromising its means and methods? And most importantly, what is the threshold above which attribution should be deemed certain?

A CRC, among other things, would provide this neutral and independent function of investigating and attributing cyberattacks without having to consider the myriad political and strategic interests that states are often prone to. The CRC would have to possess cutting-edge cybersecurity expertise, constantly improving its means and methods, to ensure that attribution is accurate and that attackers do not outsmart it and compromise its investigation and attribution functions.

3. Cybersecurity Expertise

To ensure that the global community maintained its trust in the CRC, the CRC would have to constantly be on the forefront of cybersecurity knowledge and practice. Cybersecurity offense-defense is often analogized to a cat-and-mouse game, where attackers constantly improve their techniques to overcome defensive

120. *Id.* at 409 ("[A]ttributing activity on the Internet is challenging. Hackers often route their malicious traffic through third-party proxies they either rent or compromise. An attacker in Eastern Europe that uses a botnet of compromised computers in the Middle East to conduct a DDoS attack against a U.S. target creates a false narrative that actors located in the Middle East were responsible for that act. Even attributing an attack to the actual originating computer may be insufficient; we may know the machine used to execute a hack, but not the person or group that controlled it. Thus, technical investigation must often be supplemented by credible human intelligence. And all of this must be done quickly and consistently; attribution is of little use if it takes years and only identifies a small fraction of attackers.").

121. Christopher Rosana Nyabuto, *A Game of Code: Challenges of Cyberspace as a Domain of Warfare*, 3 STRATHMORE L. REV. 49, 51 (2018).

122. However, the RAND Corporation previously proposed a global attribution agency modeled on the International Atomic Energy Agency following Microsoft's mention of the idea. *See* Milton Mueller, *A Global Cyber-Attribution Organization—Thinking It Through*, INTERNET GOVERNANCE PROJECT (June 4, 2017), https://www.internetgovernance.org/2017/06/04/a-global-cyber-attribution-org/ [https://perma.cc/SW8Y-8HQK].

123. *See* Marcus Schulzke, *The Politics of Attributing Blame for Cyberattacks and the Costs of Uncertainty*, 16 PERSP. POL. 954 (2018).

barriers created by defenders.[124] Defenders need to defend against all possible attacks and attackers,[125] while attackers only need to succeed once.[126]

Proposals for a CRC often highlight that such an institution would possess cybersecurity expertise on a global scale, a one-stop shop of sorts, which would allow states and other actors to benefit from its expertise. This expertise would exceed mere investigative and attribution assistance, focusing additionally on preventive (defensive) cybersecurity.

4. Global Norm-Creation

Next, the CRC might be able to fill in an important gap in creating global cybersecurity norms. Deep geopolitical differences between states impede the ability of international law to develop effective standards and rules for global cybersecurity. The CRC might be able to remedy this situation by developing norms and best practices that would not be influenced by geopolitical differences and unsatisfactory compromise. Rather, they would reflect the consensus of the world's professional information security community. Clearly, states set certain thresholds through treaties and customary international law—such as the existence of an armed attack or armed conflict—but the CRC could still be relevant in its ability to provide neutral standards and rules applicable in all situations, with the goal of improving information security.

5. Global Apolitical Authority

Perhaps more symbolically, the CRC will be a professional institution that is not subordinated to any state's government. This may enhance its global credibility and discourage actors from contesting its findings. However, there may need to be a mechanism in place to resolve any factual or legal disputes arising from CRC's activity.

6. The Cyber Red Cross's Utility

The idea of a CRC is a good one, but it needs to be done right. Currently, tech companies are seeking a central role in such institution, which could raise a host of

---

124. Colin Barker, *Hackers and Defenders Continue Cybersecurity Game of Cat and Mouse,* ZDNET (Feb. 3, 2016), https://www.zdnet.com/article/hackers-and-defenders-continue-cyber-security-game-of-cat-and-mouse/ [https://perma.cc/T65F-3ZZR] ("The cyber arms race between hackers and the defenders of corporate networks continues apace.").

125. WILLIS H. WARE, SECURITY CONTROLS FOR COMPUTER SYSTEMS: REPORT OF DEFENSE SCIENCE BOARD TASK FORCE ON COMPUTER SECURITY (RAND Corp. reissued 1979), https://www.rand.org/pubs/reports/R609-1.html, [https://perma.cc/43WW-9CQ7] ("The system designer must be aware of the points of vulnerability, which may be thought of as leakage points, and he must provide adequate mechanisms to counteract both accidental and deliberate events. The specific leakage points . . . [include] physical surroundings, hardware, software, communication links, and organizational (personnel and procedures).").

126. JOSEPH NYE, THE FUTURE OF POWER 125 (2011) ("Because the internet was designed for ease of use rather than security, the offense currently has the advantage over the defense.").

concerns, discussed in Part III below. The objection to the idea of a new institution for humanitarian cyberspace matters is not so much with the institution itself, but rather with the involvement of private tech companies in matters that pertain to human rights and war.

II. INTERNATIONAL LEGAL DISRUPTION

There are many international legal questions that tech companies on their own cannot practically solve,[127] nor do they have the democratic legitimacy and transparency required to do so.[128] However, tech companies are still beginning to engage in creating international norms and rules to address security issues arising in cyberspace. On top of that, their relative degree of uncontested success in creating such norms and rules is due to states' inability to bridge geopolitical divides, making it unlikely that states will reach a consensus on how to regulate cybersecurity globally in the near future.[129] Tech companies have decided to take on that role.

International law, at least traditionally, involves norms and rules created by states, either through their explicit consent in treaties or through custom developed through the years which states consider to be legally binding.[130] Formally speaking, the three authoritative instruments that make up international law are treaties, custom, and general principles.[131] Judicial decisions (such as the International Court of Justice's) and legal scholarship reflect subsidiary sources for determining the rules of international law.[132]

Currently, there is no universal treaty on how cybersecurity relates to civilians,[133] nor is there a prevailing and long-standing custom that could inform states of the best practices and red lines applicable to their offensive and defensive

---

127. Pamela Lian, *'Digital Geneva Convention'? What's Next for Internet Governance Challenges?*, ITU NEWS (Nov. 13, 2017), https://news.itu.int/digital-geneva-convention-whats-next-for-internet-governance-challenges/ [https://perma.cc/9J7J-VCGZ] ("Neither national governments, nor the technology sector, nor civil society, nor anyone else can alone solve the challenges of technological progress.").

128. Kenneth A. Bamberger & Orly Lobel, *Platform Market Power*, 32 BERKELEY TECH. L.J. 1051, 1084 (2017) ("[T]he major antitrust concerns surround the control of data by a small number of concentrated companies and the lack of transparency about their collection and usage."); *see also* Jacob Kasternakes, *FCC Chairman Says Twitter, Facebook, Google May Need Transparency Law*, VERGE (Sept. 4, 2018, 2:20 PM), https://www.theverge.com/2018/9/4/17819418/fcc-chairman-web-company-transparency-regulation-pai [https://perma.cc/JDW6-VYB8] ("The leader of the Federal Communications Commission says that major web companies like Facebook, Twitter, and Google have offered little transparency into how they work—and it's time to seriously consider forcing them to tell us.").

129. *See* GOLDSMITH, *supra* note 2.

130. Brown & Poellet, *supra* note 44, at 126 ("The body of international law is a jumble of historic practice and tradition as well as signed agreements between nations.").

131. Statute of the International Court of Justice art. 38(1), June 26, 1945, 59 Stat. 1055, 33 U.N.T.S. 993.

132. *Id.* art. 38(1)(d).

133. *See* Ido Kilovaty & Itamar Mann, *Towards a Cyber-Security Treaty*, JUST SECURITY (Aug. 3, 2016), https://www.justsecurity.org/32268/cyber-security-treaty/ [https://perma.cc/P8KT-6ZWS] (arguing that a cyber-specific treaty is needed to protect civilians and institutions).

use of cyberspace.[134] There seems to be a major geopolitically- and ideologically-based disagreement among states as to what these practices and red lines should be, particularly between the states that are principally involved in cyberspace and thus benefitting from its use: the United States, United Kingdom, Russia, China, Israel, and Iran, to name a few.[135]

It therefore comes as no surprise that corporations have taken charge in arguing for an amendment to and reevaluation of existing international law norms and rules that fail to provide reasonable protections for civilians in cyberspace. Microsoft's attempts to promote a Digital Geneva Convention that would extend to peacetime the protections afforded to civilians during wartime is one example of such involvement.

This Part looks at states' current international endeavors to develop frameworks for regulating global cybersecurity. As this Article has argued, these attempts have largely failed. As a consequence, private tech companies are taking over. This Part looks at what exactly these norms are and how they may end up regulating international relations in the cybersecurity context. Finally, it looks at whether these developments represent a normative crisis.

A. International Legal Failure

Why does international law fail to regulate state conduct in cyberspace? There may be many compelling answers to this question. Perhaps there is disagreement over how some legal terms of art apply in cyberspace. For example, what is an "attack"[136] or a "use of force" in cyberspace?[137] There is certainly some practical difficulty in attempting to apply territorial concepts to an aterritorial space.[138] The

134. Dan Efrony & Yuval Shany, *A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice*, 112 AM. J. INT'L L. 583, 595 (2018) (arguing not only that there isn't any current state practice on the matter, but that it is unlikely one will evolve anytime soon: "The lack of transparency in the field—underreporting of cyberoperations and limited attribution claims—makes it difficult to identify relevant state practice").

135. Sintia Radu, *China, Russia Biggest Cyber Offenders*, U.S. NEWS (Feb. 1, 2019, 5:30 PM), https://www.usnews.com/news/best-countries/articles/2019-02-01/china-and-russia-biggest-cyber-offenders-since-2006-report-shows [https://perma.cc/EF9U-2SB4] (citing a report studying the most active countries in cyber offense, which "examined data on China, North Korea, Iran, India, Russia, the United Kingdom, the United States, Germany, Australia, Japan, South Korea, Ukraine, Israel and France").

136. Protocol I, *supra* note 41, at art. 49(1), 1125 U.N.T.S. at 36 (defining "attacks" as "acts of violence against the adversary, whether in offense or in defense"). For a thorough discussion and analysis of which offensive uses of cyberspace constitute an "attack" and how an "attack" ought to adapt to the realities of cyber offense, see Kilovaty, *supra* note 47.

137. *See* U.N. Charter art. 2(4); *see also* Kim Zetter, *Legal Experts: Stuxnet Attack on Iran Was Illegal 'Act of Force'*, WIRED (Mar. 25, 2013, 12:53 PM), https://www.wired.com/2013/03/stuxnet-act-of-force/ [https://perma.cc/E9QG-F5CC] (arguing that the Stuxnet worm unleashed against the Iranian nuclear program may have violated Article 2(4) of the U.N. Charter prohibiting the use of force). *See generally* Matthew Waxman, *Cyber Attacks as "Force" Under UN Charter Article 2(4)*, 87 INT'L L. STUD. 43 (2011).

138. *See, e.g.*, Jennifer Daskal, *The Un-Territoriality of Data*, 125 YALE L.J. 326, 379 (2015) (observing that data is "unterritorial").

issue may also be about boundary-setting. We know that international law protects state sovereignty, but how far does that sovereignty extend in cyberspace?[139] Also, international humanitarian law allows a certain degree of collateral damage to civilians and civilian objects. But does damage to data fall within the scope of "civilian objects"?[140] Or, perhaps the reason is far more grounded in realism than anyone can imagine, with states seeking to keep their power to clandestinely and effectively engage in state-to-state offensive activity in cyberspace.[141] In this context, cyberspace would be a legal *terra incognita*, where the legal aspects of state activity in cyberspace is not only unexplored but also undesirable from the states' points of view.[142]

Indeed, the work of Dan Efrony and Yuval Shany suggests that states, particularly those significantly engaged in cyberspace, are reluctant to accept legally binding rules for their conduct because they have "a limited interest in promoting legal certainty regarding the regulation of cyberspace."[143] This suggests that there is nothing structurally flawed with the law, but rather the challenge is with states who wish to retain their authority and power by resisting the infusion of cyberspace with legal standards and rules. It therefore comes as no surprise that tech companies are taking over a role that the international community is unable to perform.

Kubo Mačák's work on the crisis of international law and cybersecurity is equally alarming.[144] Mačák identifies three trends that together support his assertion that international law has not only failed to regulate cybersecurity, but also that we are in an actual crisis.[145] First, there are no attempts to codify the rules applicable to global cybersecurity in a binding treaty.[146] Second, states are reluctant to develop binding customary international law.[147] And, third, whatever multilateral processes

---

139. Gary P. Corn & Robert Taylor, *Sovereignty in the Age of Cyber*, AM. J. INT'L L. UNBOUND 207, 210 (2017) ("The principle of sovereignty is universal, but its application to the unique particularities of the cyberspace domain remains for states to determine through state practice and/or the development of treaty rules.").

140. *See, e.g.*, Heather Harisson Dinniss, *The Nature of Objects: Targeting Networks and the Challenge of Defining Cyber Military Objectives*, 48 ISR. L. REV. 39, 45 (2015) (arguing that data should be recognized as object to better protect civilians); Kubo Mačák, *Military Objectives 2.0: The Case for Interpretive Computer Data as Objects Under International Humanitarian Law*, 48 ISR. L. REV. 55, 55 (2015) (arguing that data ought to be an 'object'); Michael Schmitt, *The Notion of 'Objects' During Cyber Operations: A Riposte in Defence of Interpretive and Applicative Precision*, 48 ISR. L. REV. 81, 84 (2015) (arguing that data should not be characterized as an object in itself).

141. Dan Efrony, *Is It Time to Regulate Cyber Conflicts?*, LAWFARE (May 4, 2018, 7:00 AM), https://www.lawfareblog.com/it-time-regulate-cyber-conflicts [https://perma.cc/6N4N-QW7D] ("The legal and political ambiguity coupled with the power to act covertly benefits the most technologically capable nations in cyberspace, and those nations won't voluntarily give away their newly acquired strategic superiority.").

142. *Id.*

143. Efrony & Shany, *supra* note 134, at 585.

144. Kubo Mačák, *Is the International Law of Cyber Security in Crisis?*, 8 INT'L CONF. CYBER CONFLICT 127 (2016).

145. *Id.*

146. *Id.* at 129–30.

147. *Id.* at 130.

still take place, their focus tends to be on nonbinding norms.[148] What follows is a review of some of the most prominent processes and efforts to establish the international rules for global cybersecurity.

1. U.N. Group of Governmental Experts

The United Nations' Group of Governmental Experts (GGE) was an effort to create and clarify rules of conduct in cyberspace. The U.N. GGE was established in 1999 to consider "Developments in the Field of Information and Telecommunications in the Context of International Security."[149] The GGEs consisted of fifteen to twenty representatives of member states who would examine an issue and report back to the General Assembly if they were able to come to a consensus agreement on a report. Three of these GGEs were successful in producing such reports, in 2010, 2013, and 2015.

The project gained the favor of the G-7,[150] G-20,[151] and the OECD,[152] and appeared to be on the right track to achieve something truly revolutionary[153]: a comprehensive set of rules clarifying and constraining transnational state behavior in cyberspace. The apex of this endeavor was in 2015, when the GGE released a report containing a series of rules that was seemingly uncontroversial, representing what appeared to be a strong consensus.[154] For example, the report suggested that a state should "not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public."[155] Even though GGE Reports rules are voluntary and nonbinding, states did not accept these recommendations and the project collapsed

148. *Id.* at 131.

149. G.A. Res. 53/70, Developments in the Field of Information and Telecommunications in the Context of International Security (Jan. 4, 1999) ("Calls upon Member States to promote at multilateral levels the consideration of existing and potential threats in the field of information security.").

150. *The Year in Review: The Death of the UN GGE Process?*, COUNCIL FOREIGN REL. (Dec. 21, 2017), https://www.cfr.org/blog/year-review-death-un-gge-process [https://perma.cc/MW4J-EJCY].

151. *Id.*

152. *Id.*

153. *See* Joseph Marks, *U.N. Body Agrees to U.S. Norms in Cyberspace*, POLITICO (July 9, 2015, 12:44 PM), https://www.politico.com/story/2015/07/un-body-agrees-to-us-norms-in-cyberspace-119900 [https://perma.cc/9BRD-KMW2] ("It's a breakthrough for U.S. diplomats, who have been pushing these 'norms' as an alternative to formal treaties as a way to help tame the lawless frontier of cyberspace.").

154. Elaine Korzak, *The 2015 GGE Report: What Next for Norms in Cyberspace?*, LAWFARE (Sept. 23, 2015, 8:32 AM), https://www.lawfareblog.com/2015-gge-report-what-next-norms-cyberspace [https://perma.cc/VWA9-FB35].

155. Rep. of the Grp. of Governmental Experts on Devs. in the Field of Info. and Telecomms. in the Context of Int'l Sec., transmitted by letter dated 26 June 2015 from the Chair of the Grp., U.N. Doc. A/70/174, at 8 (July 22, 2015).

entirely at the GGE's last session in June 2017.[156] As one commentator put it, "a nearly seven-year process to write the rules that should guide state activity in cyberspace came to a halt."[157] Many attribute this failure to inevitable geopolitical differences between the United States, Russia, and China.[158] This divide is rooted in two different disagreements: whether the use of cyber operations should be allowed at all[159] (regulation vs. a complete ban) and which activities constitute cyber conflict to begin with.[160]

This failure at the U.N.—the most international forum for states to negotiate new regimes—created a normative vacuum that is likely to be usurped by other, nongovernmental stakeholders: tech companies. Tech companies realize that states were, are, and will be unable to reach a consensus, and that the normative and geopolitical divide will only continue to deepen moving forward.

2. The Tallinn Manual

Unlike the U.N. GGE process, the *Tallinn Manual*[161] was comprised of a group of academics focused on how current law applies to cyber operations.[162] There was no ambition to create new rules, regimes, or norms. The project was pretty straightforward. The experts were to identify the law as it is at present (*lex lata*) and apply that law to a new phenomenon: cyber operations.[163]

---

156. Arun Sukumar, *The UN GGE Failed. Is International Law in Cyberspace Doomed as Well?*, LAWFARE (July 4, 2017, 1:51 PM), https://www.lawfareblog.com/un-gge-failed-international-law-cyberspace-doomed-well [https://perma.cc/2XS7-T2LH].

157. Grigsby, *supra* note 53, at 109.

158. Elaine Korzak, *UN GGE on Cybersecurity: The End of an Era?*, DIPLOMAT (July 31, 2017), https://thediplomat.com/2017/07/un-gge-on-cybersecurity-have-china-and-russia-just-made-cyberspace-less-safe/ [https://perma.cc/2X4F-HY2L] (explaining in detail the reasons for the disagreement between Russia, China, Cuba, and the United States).

159. Grigsby, *supra* note 53, at 113–14 ("While Washington wanted to further develop how concepts such as neutrality, proportionality and distinction might constrain cyber conflict, Moscow and Beijing saw Washington trying to find justifications in international law for the use of cyber means during a conflict or of conventional means as a way to respond to cyber conflict, leading to destabilising activity. Russian and Chinese diplomats wanted to concentrate their efforts on preventing cyber-based conflict in the first place, instead of setting the rules for something that should not be allowed to happen.").

160. *Id.* at 114 ("China, Russia and the United States fundamentally disagree over the nature of cyber conflict itself. Washington views cyber security as the protection of bits, software and hardware from unauthorised use—such as manipulating data, accessing confidential data or making data unavailable. In contrast, Beijing and Moscow prefer the term 'information security', which allows for state control over online content so as to preserve regime stability.").

161. TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS (Michael N. Schmitt & Liis Vihul eds., 2017) [hereinafter TALLINN MANUAL 2.0].

162. *Id.* at 3 ("*Tallinn Manual 2.0* examines key aspects of the public international law governing 'cyber operations.'").

163. *Id.* ("*Tallinn Manual 2.0* is intended as an objective restatement of the *lex lata*. Therefore, the Experts involved in both projects assiduously avoided including statements reflecting *lex ferenda*.")

The process resulted in two separate manuals. The first, released in 2013, focused narrowly on the international regulation of warfare.[164] Questions of what constitutes a "use of force,"[165] an "attack,"[166] and a "civilian"[167] were commonplace in the first *Tallinn Manual*. But this narrow approach, while relevant in armed conflict situations, misses a substantial chunk of state activity in cyberspace. Espionage,[168] disruption,[169] election interference,[170] manipulation, and disinformation are just a few examples of widespread activities that would not be covered by warfare regulation, simply because they do not constitute war.

This understanding led to the *Tallinn Manual 2.0*, released in 2017. This iteration broadened its methodology to include law relevant to cyber operations below the threshold of war. This included questions such as, at what point does a cyber operation violate the norm on nonintervention?[171] How is sovereignty conceptualized in cyberspace?[172] To what extent does human rights law protect Internet users from harmful state-sponsored activity?[173]

While the experts participating in the *Tallinn Manual* project were able to reach consensus on how the law applies to cyber operations, acceptance of the Tallinn Manual was very thin, to say the least. Dan Efrony and Yuval Shany found that there was "limited support in state practice for certain key Rules of the *Tallinn Manual*, and that it is difficult to ascertain whether states accept the *Tallinn* Rules and wish them to become authoritative articulations of international law governing cyberoperations."[174] In other words, the *Tallinn Manual*, while creating a comprehensive and plausible set of rules, has failed in securing the acceptance of the international community.

3. Other Processes

There are several other ongoing and prospective processes that revolve around the creation of norms for state behavior in cyberspace. The Dutch-sponsored

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

165. *Id.* at 42.

166. *Id.* at 106–10 (rule 30).

167. *Id.* at 104–05 (rule 29).

168. TALLINN MANUAL 2.0, *supra* note 161, at 168 ("Although peacetime cyber espionage by States does not per se violate international law, the method by which it is carried out might do so.").

169. *Id.* at 312–27.

170. *Id.* at 313 ("This Rule addresses situations in which a State intervenes by cyber means in the 'internal or external affairs'. . . . [F]or example, by using cyber operations to remotely alter electronic ballots and thereby manipulate an election.").

171. *Id.* at 312.

172. *Id.* at 11.

173. *Id.* at 179–208.

174. Efrony & Shany, *supra* note 134, at 585.

Hague Process facilitates state follow-up on the *Tallinn Manual 2.0* through an input process, training, and state consultation.[175]

The Global Commission on the Stability of Cyberspace is another nongovernmental project focused on the development of norms and rules to promote international peace and security in cyberspace.[176] It focuses on "reaching new universal agreements on substantive standards for state behavior."[177]

B. From State-Centric to Tech-Centric Legal Order

Many tech companies are becoming involved in initiatives tasked with creating norms, rules, principles, and guidelines for different technological conundrums. This trend reflects a new concept of how rules on technology are created. If in the past we expected state governments to perform their roles by legislating, regulating, creating norms, and governing, this basic premise is changing rather quickly with the emergence of new technologies and complex issues in cyberspace. This trend has two key characteristics. First, tech companies create norms. Second, these norms apply to the conduct of states.

1. Norms Created by Tech Companies

Perhaps the main evolutionary aspect in how global cybersecurity norms are being created is that private tech companies are the entities coming up with them. But private tech companies are not legislators in the classic sense, though scholars like Joel Reidenberg and Lawrence Lessig make it clear that architecture, or code, is in fact a method of regulation in cyberspace.[178] It is worth remembering that these code regulators are for-profit corporations that seek to benefit their bottom line. Many of the challenges with this form of norm creation derive from tech exceptionalism and the inherent identity and motivation of private for-profit corporations: profit seeking.

---

175. Michael Schmitt & Liis Vihul, *International Cyber Law Politicized: The UN GGE's Failure to Advance Cyber Norms*, JUST SECURITY (June 30, 2017), https://www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms/ [https://perma.cc/2ZPQ-W7XQ].

176. GLOBAL COMMISSION ON THE STABILITY OF CYBERSPACE, https://cyberstability.org/ [https://perma.cc/6FKY-349R].

177. Duncan Hollis & Matthew Waxman, *Promoting International Cybersecurity Cooperation: Lessons from the Proliferation Security Initiative*, 32 TEMP. INT'L & COMP. L.J. 147, 149 (2018).

178. *See* Joel Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules through Technology*, 76 Tex. L. Rev. 553, 554 (1998) ("[L]aw and government regulation are not the only source of rulemaking. Technological capabilities and system design choices impose rules on participants."); *see also* LAWRENCE LESSIG, CODE VERSION 2.0, at 79 (2006) ("As the world is now, code writers are increasingly lawmakers. They determine what the defaults of the Internet will be; whether privacy will be protected; the degree to which anonymity will be allowed; the extent to which access will be guaranteed. They are the ones who set its nature. Their decisions, now made in the interstices of how the Net is coded, define what the Net is.").

Microsoft and other tech companies are not new to government-like roles. They are already undertaking many governmental and quasi-governmental tasks. For example, Microsoft is engaged in a public-private partnership with the U.S. government to take down botnets around the world.[179] While some would certainly argue that this sort of public-private partnership is a success in that the U.S. government is able to fight cybercrime with the assistance of the prowess of a private tech company, others are concerned about the public values that are implicated with private companies performing certain government-like functions.[180] However, these partnerships, which the government often initiates and leads, are different from the phenomenon of tech companies independently creating norms with no substantial governmental or public oversight.

2. Norms Applicable to State Conduct

Private tech companies create norms, which are largely applicable to their own business activities. However, with the emerging privatization of cyberspace law, we begin to see that these norms also apply to the conduct of states in cyberspace, whether in offense or defense. For example, the "neutrality" principle which tech companies currently promote has to do with how these companies ought to treat states requesting assistance in carrying out cyberattacks. Under the neutrality principle, tech companies will treat requests from all states equally, regardless of the identity of the state requesting assistance. Under such neutrality, they will treat requests for assistance from the U.S. government, the Chinese government, the Russian government, or any other, indiscriminately.

This, perhaps, does not represent a very new approach to how states seek expertise and assistance in carrying out certain military, law enforcement, and at times political operations. Rather, tech companies that have historically been complacent and subservient to the states' desires are now becoming more restrictive and methodical on what sort of assistance and information they agree to provide to states.

The positive consequence of tech companies setting the rules of the game is that this pushes back on certain regimes' abuses of power and authoritarianism. Many tech companies have realized that to protect their consumers everywhere, they need to restrict state governments and their access to and control of online platforms, tools, and resources.

While it is certainly desirable that tech companies reduce abuse and harmful state activity in cyberspace, the more problematic aspect of this trend is that states are ceding a lot of control to tech companies that do not share the same

179. Zach Lerner, *Microsoft the Botnet Hunter: The Role of Public-Private Partnerships in Mitigating Botnets*, 28 HARV. J.L. & TECH. 237, 250–58 (2014) (reviewing the history and legitimacy of the United States-Microsoft public-private partnership on botnet takedowns).

180. *See* Eichensehr, *supra* note 12, at 504–05.

accountability, legitimacy, and transparency[181] values as state governments, particularly those elected by the public.[182] In other words, international lawmaking is being unintentionally delegated to private tech companies.

C. A Normative Crisis

Tech companies' ability to restrict state governments worldwide has many positive aspects, but it also reflects a larger flow in the redistribution of power in cyberspace from states to tech companies.[183] International law was traditionally created by states, for states. Some changes over time led to more norms and laws addressed at humans and their rights vis-à-vis their governments: human rights law. There are also many examples of "bottom-up" international lawmaking, but nothing of the scale and effect that tech companies' ability to create law may have on cyberspace and the global legal order. This privatization of cyberspace law may become serious and consequential if states, the public, civil society organizations, and other stakeholders do not step back to consider the ramifications.[184]

III. A NEW LEGAL ORDER

We are about to see a new legal order around cyberspace and technology. Tech companies are not merely focused on one technology or one cyberspace issue, but they rather want to assimilate themselves into the machine that produces law. Some would argue that tech companies are performing a role that states will never be able to: regulating cyberspace and new technologies. Indeed, there are many indications that states lag behind in regulating and containing the risks of new technologies. But at the same time, these same states are constrained by public values and norms that mandate transparency, fairness, accountability, and more. States, while imperfect in dealing with emerging issues in cyberspace, are under a whole different set of normative pressures.

This Part consists of two sections. The first explores the different values that typically govern state action and may therefore need to be assessed with respect to the privatization of cybersecurity law. The second makes some observations with regard to future private lawmaking on technology-related matters, calling for state

181. *Id.* at 506 ("Government actions are also subject to scrutiny through mechanisms such as freedom-of-information requests and investigations by Congress or agency inspectors general.").

182. *Id.* at 505–06 ("Governmental actors operate in a system of structural checks that, although imperfect, constrains their actions. Government officials may be held accountable through congressional oversight and elections either of themselves or of higher level officers who are responsible for the actions of the bureaucracy.").

183. *Id.* at 504 ("The increasing transfer of government functions to private actors in recent decades has sparked academic and popular debate about privatization.").

184. Hurel & Lobato, *supra* note 110, at 62 (recognizing the difficulty of platforms having a monopoly on what they refer to as norm entrepreneurship, urging the participation of other stakeholders as well: "Cybersecurity is best understood as a process triggered by the practices of different actors, namely markets, think tanks, IT communities, governments, and security experts").

governments, civil society, and Internet users to take collective action to demand certain safeguards to the values laid out in this Part.

A. Privatized Cybersecurity Law & Values

The privatization of cybersecurity law requires an in-depth examination of the public law values affected by the tech industry's usurpation of the global legislative role.[185] These values evolved as a measure to constrain governments' power and overreach.[186] Generally, private entities were not considered to be menacing to individual freedoms and other structural and normative principles such as accountability and transparency. But these values are either absent or significantly jeopardized when tech companies are performing a governmental function,[187] as "private interests are often at odds with public law values."[188] The values discussed here are democratic legitimacy, transparency, privacy, neutrality, and parity.

1. Democratic Legitimacy

Typically, when legislatures create laws and regulators promulgate regulations, they enjoy a certain degree of legitimacy. However, tech companies do not possess an equivalent legitimacy in creating law and norms for cyberspace. Yet, the tech sector still creates rules and norms without it. It can do so because international law recognizes custom as an acceptable and primary source of law.[189]

We have seen statements reflecting this notion. Mark Zuckerberg claimed that, "[i]n a lot of ways Facebook is more like a government than a traditional company. We have this large community of people, and more than other technology companies we're really setting policies."[190]

Statements and responses such as these empower platforms to pursue quasi-legislative functions. State governments are not even necessarily pushing back.

---

185. *See generally* Eichensehr, *supra* note 12.

186. Laura Dickinson, *Public Law Values in a Privatized World*, 31 YALE J. INT'L L. 383, 397, 400 (2006) ("[T]he protections contained in the U.S. Constitution are generally viewed as prohibitions on state misconduct only . . . . Thus, widespread privatization potentially threatens a wide variety of public law values.").

187. However, some would argue that administrative law has long been informing the tech industry on how to self-regulate in a way that replicates public governance. *See* Kate Klonick, *The New Governors: The People, Rules, and Processes Governing Online Speech*, 131 HARV. L. REV. 1598, 1663 (2018) ("[A]dministrative law . . . has long implicated the motivations and systems created by private actors to self-regulate in ways that reflect the norms of a community.").

188. *See* Eichensehr, *supra* note 12, at 535.

189. Jurich, *supra* note 50, at 292 ("The inclusion of nonstate voices in the process allows for the potential of a bottom-up lawmaking process that may identify and negotiate around factors that private actors value.").

190. DAVID KIRKPATRICK, THE FACEBOOK EFFECT: THE INSIDE STORY OF THE COMPANY THAT IS CONNECTING THE WORLD 254 (2010).

The Danish government recently appointed an ambassador whose role is simply to deal with powerful tech companies such as Facebook and Google.[191]

This calls into question a variety of other concerns deriving from the illegitimacy of the tech sector's endeavors. For example, what are the *real* interests behind the rules and norms prescribed by the tech sector? What degree of transparency should the tech sector provide when it creates, enforces, interprets, and amends its own rules and norms? Is the tech sector at all accountable, and if so, to whom?

2. Transparency

Transparency is often raised by scholars as one of the central values that tech companies ought to embrace.[192] The argument goes that if tech companies are transparent in what, how, and why they do certain things, this may alleviate the information gap between them and consumers. While the importance of transparency in tech cannot be overstated, the obsession with transparency misses the bigger picture, which is that tech companies simply want to govern. The desire to govern is unlikely to disappear even if we achieve full transparency, because it is rooted in a desire for power.

Janosik Herder, for example, suggests that we should look at tech companies as "biopolitical companies."[193] These biopolitical companies want to "govern populations" which:

> puts them at odds with democratic states that were historically thought to be the primary loci of biopower. Whereas the rise of platforms has consistently been greeted with enthusiasm for their democratizing potential, it may now be time to start to be concerned about the power platforms wield and what their power means for democratic states.[194]

Transparency is important. The tech industry needs to be sincere about how it comes up with its proposed rules and norm for cyberspace, but this sincerity does not address the core issue that this Article focuses on: power. Or, more specifically, how power over global cybersecurity regulation is inadvertently shifting from states to tech companies.

3. Privacy

The ability of tech companies to regulate global cybersecurity raises various privacy-related questions, such as, what sort of data will tech companies collect

---

191. Adam Taylor, *Denmark Is Naming an Ambassador Who Will Just Deal with Increasingly Powerful Tech Companies*, WASH. POST (Feb. 4, 2017, 12:30 AM), https://www.washingtonpost.com/news/worldviews/wp/2017/02/04/denmark-is-naming-an-ambassador-who-will-just-deal-with-increasingly-powerful-tech-companies/ [https://perma.cc/GYX2-WAD3].

192. *See, e.g.*, Klonick, *supra* note 187, at 1665 ("[T]here is very little transparency from these private platforms.").

193. Herder, *supra* note 4.

194. *Id.*

while acting as the guardians of cyberspace? If an industry-led CRC is to be established, how will it collect, use, and secure sensitive and valuable data? The question of privacy is overlooked in the frameworks that tech companies attempt to promote. There is a lot to gain from this unprecedented access to valuable data globally. Tech companies have an incentive to use this data for commercial purposes, as their cybersecurity mission also happens to be their business mission.

Whether tech companies can respect privacy and secure the confidentiality of our personal information is a question of trust.[195] Recent privacy violation scandals involving Facebook and other tech companies had negative implications on the trust that users are willing to afford to tech companies.[196]

Privacy is not only important for its inherent value, but also because tech companies thrive on data and therefore have an incentive to collect and understand as much of it as possible.[197] Frank Pasquale observes that "platforms are now leveraging data advantage into profits, and profits into further domination of advertising markets. The dynamic is self-reinforcing: more data means providing better, more targeted services, which in turn attracts a larger customer base, which offers even more opportunities to collect data."[198] This may explain the incentive that many tech companies have in participating in different regulatory regimes that can enhance their access to consumer data.

4. Neutrality

Can tech companies truly be neutral vis-à-vis state governments? The Cybersecurity Tech Accord contains a promise that the undersigned "will not help governments launch cyberattacks against innocent citizens and enterprises from anywhere."[199] As Kristen Eichensehr puts it, these tech companies "cast themselves as neutrals amidst competing claims by national governments and in the face of claims by the U.S. government for preferential treatment because of their status as U.S. companies."[200] Andrew Woods explains that this sort of neutrality is more strategic than ideological, and temporary rather than permanent.[201]

The San Bernardino terrorist attack, which culminated in a dispute between the FBI and Apple as to the extent of assistance that Apple owed the FBI in its

195. ARI EZRA WALDMAN, PRIVACY AS TRUST: INFORMATION PRIVACY FOR AN INFORMATION AGE 4 (2018) ("[B]ecause we share when we trust, I argue that we should start talking about, thinking through, and operationalizing information privacy as a social norm based on trust.").

196. Marietje Schaake, *Beware of Tech Companies Playing Government*, BLOOMBERG (Jan. 16, 2019, 10:00 PM), https://www.bloomberg.com/opinion/articles/2019-01-17/beware-of-tech-companies-playing-government [https://perma.cc/T9QV-S98R] ("If we've learned anything from the scandal after scandal over Facebook Inc's handling of user data, it is that the private sector's noble intentions to regulate the internet should be met with skepticism. Without adequate public oversight of algorithms, and with recurring bad practices, tech platforms cannot—should not—be trusted.").

197. Pasquale, *supra* note 5, at 3.

198. *Id.*

199. *A Digital Geneva Convention to Protect Cyberspace*, *supra* note 54.

200. Eichensehr, *supra* note 69, at 698.

201. Woods, *supra* note 111, at 5.

investigation, illustrates the need for neutrality. Apple may have many reasons why it cannot or would not help the FBI, but one of them should be that Apple will not give U.S. authorities preferential treatment over any competing demands from other state governments.[202]

The question remains whether this neutrality is aspirational or practical in reality. U.S.-based companies are still subject to U.S. laws and regulations. Tech companies who operate in other foreign markets are similarly subjected to local laws and regulations applicable to their activity.[203] It is therefore unclear whether this neutrality can be achieved, and if so, at what price to law enforcement and other state interests.

5. Parity

The last concern is that of parity, looking to the power dynamics between states and tech companies. Kristen Eichensehr asks whether tech companies are becoming on par with countries and says that, if this were the case, it would be "potentially revolutionary."[204] Eichensehr then reviews the qualities that we tend to associate with Westphalian sovereigns and concludes that, despite similarities to states, companies have not achieved perfect parity.[205] This conclusion is largely based on the fact that tech companies lack territory,[206] coercive power,[207] recognition,[208] and are still "subordinate to public authorities and legal regimes within the states in which they operate."[209] Similarly, Andrew Woods argues that tech companies pose no challenge to state sovereignty at all.[210] According to Woods, states can assert their sovereignty whenever tech companies push too far.[211] These views miss the bigger picture, and I respectfully disagree.

It is misguided to compare what tech companies are doing nowadays to the concept of Westphalian sovereignty, which dates back to the 1648 Peace of Westphalia. No one back then anticipated that private corporations would one day become so powerful that their power would not even fall within the ideas of sovereignty conceived at Westphalia. It is true that tech companies lack the characteristics Eichensehr lays out, but it does not necessarily follow that they are not on par with states.

---

202. *See* Eichensehr, *supra* note 69, at 698.
203. *Id.* at 699.
204. *Id.* at 685.
205. *Id.* at 694.
206. Montevideo Convention on Rights and Duties of States art. 1, Dec. 26, 1933, 165 L.N.T.S. 19 ("The state as a person of international law should possess the following qualifications: a) a permanent population; b) a defined territory; c) government; and d) capacity to enter into relations with the other states.").
207. *See* Eichensehr, *supra* note 69, at 684.
208. *Id.* at 695.
209. *Id.*
210. Woods, *supra* note 111.
211. *Id.* at 6.

However, despite tech companies' power, they are not on an equal footing with states because we should use different metrics of sovereignty for *states* and *tech companies*. It is unlikely that tech companies will ever have independent territories like states, but they will become increasingly powerful despite their aterritorial nature. These tech companies own cyberspace "territories," market shares, and industry monopolies, which may be even more significant than physical territory in the cybersecurity context. And while it is true that tech companies do not have a monopoly on the use of force, they do often act in monopolistic ways in cyberspace which states would not be able to. Finally, tech companies are indeed subject to the laws and regulation in markets where they operate, but the ability of these markets to reshape how tech companies operate *globally* is somewhat limited. Yes, nation *Y* can pass legislation to restrict the user data that platform *X* can collect and use. But nation *Y* cannot pass legislation that will change platform *X*'s business and policy strategy throughout the entire world.[212] This is a collective action problem of sorts.

The question of parity, therefore, is not whether tech companies are states or whether they have territory. Rather, it is about tech companies becoming powerful in their own unique way, which challenges the notions of power and coercion that we typically associate with states. Tech companies do not have territories, armies, or recognition as sovereign states, but their emerging power represents a new type of sovereignty—digital rather than Westphalian. As Frank Pasquale has observed, the tech companies' increase in power represents a "shift from territorial to functional sovereignty."[213]

B. The Future of Privatized Tech Legislation

Privatized cybersecurity law represents a single instance of tech companies assuming a role in regulating global cybersecurity. However, this is part of a broader phenomenon that has implications for future platform-sponsored initiatives to create law on tech-related matters.

The phenomenon of privatized cybersecurity law may herald a broader phenomenon of privatized legislation, where tech companies engage in the creation of norms and rules that would benefit their private interests. That does not necessarily mean that Internet users or other consumers would suffer, but it signals that lax government control of these initiatives will jeopardize the public law values discussed *infra*.

This increase in privatization is reflected in Amazon and Microsoft's recent move to promote facial recognition legislation that "protects individual civil rights and ensures that governments are transparent in their use of facial recognition

212. Sarah Marsh, *'Right to Be Forgotten' on Google Only Applies in EU, Court Rule*, GUARDIAN (Sept. 24, 2019), https://www.theguardian.com/technology/2019/sep/24/victory-for-google-in-landmark-right-to-be-forgotten-case [https://perma.cc/RN4E-VXXK] (explaining when the European Court of Justice held that while the right to be forgotten is part of data protection law in the EU, it will only apply within the territory of the EU).

213. Pasquale, *supra* note 5, at 2.

technology."[214] This does not necessarily suggest that tech companies will become any more involved in shaping technology regulation than they have been in the past, but rather that they will reframe their methodology. Instead of lobbying for a certain agenda with legislators and regulators, tech companies will now independently offer "norms," "principles," and "guidelines" for technologies that they themselves develop. This will further blur the lines between government-sponsored legislation and platform-created norms, which will frustrate challenges to or public oversight of these norms.

In addition, the privatization of tech law, which is currently the creation of mostly U.S.-based tech companies, will further exacerbate the current distrust among governments who seek to leverage their cyber offense. These governments may feel as if these corporate initiatives are hegemonic, under-representative, and therefore illegitimate.[215] These privatized laws could potentially be seen as U.S.-sponsored norms that seek to imperialize global norms without going through the proper international lawmaking processes.

CONCLUSION

This Article demonstrates the tech industry's growing involvement in creating and promoting international norms and rules for global cybersecurity. While the case studies in this Article focus on cybersecurity, this involvement is extending into other areas of technology regulation, such as facial recognition, data privacy, and more.

The tech industry is therefore assuming the informal role of global cybersecurity legislator. This privatization of cybersecurity law is one example out of many, reflecting the broader governmentalization of the private tech industry. Other stakeholders ought to be responsive to this phenomenon in order to avoid abuse by tech companies. As Yafit Lev-Aretz and I observed a few years ago, "if it talks like a government and acts like a government, it must be a tech giant."[216]

Tech companies are now using the normative vacuum left by states to step in and promote their own vision of global cybersecurity norms. This involves not only the promulgation of norms, but also the creation of institutions such as a Cyber Red Cross. As this Article demonstrated, this privatization of cybersecurity law has created some opportunities but also raised considerable issues that state governments, civil society actors, and Internet users need to be cognizant of. While

---

214. Tom Simonite, *Amazon Joins Microsoft's Call for Rules on Facial Recognition*, WIRED (Feb. 7, 2019, 6:47 PM), https://www.wired.com/story/amazon-joins-microsofts-call-rules-facial-recognition/ [https://perma.cc/Q5PK-HLKQ].

215. *See* Hollis & Waxman, *supra* note 177, at 156 (explaining how the Proliferation Security Initiative, which the authors consider a plausible model for global cybersecurity, was often perceived as hegemonic and under-representative).

216. Ido Kilovaty & Yafit Lev-Aretz, *If It Talks like a Government and Acts like a Government, It Must Be a Tech Giant*, TECHCRUNCH (Mar. 31, 2017, 1:00 PM), https://techcrunch.com/2017/03/31/if-it-talks-like-a-government-and-acts-like-a-government-it-must-be-a-tech-giant/ [https://perma.cc/5PT2-QW4E].

the tech industry has an important role to play in global cybersecurity, state governments would be wise to curb the appetite for power that some of the major tech companies currently have, so that values such as democratic legitimacy, accountability, and transparency can be effectuated. This requires further global efforts of creating authoritative norms through multi-stakeholder processes that involve a diverse set of legitimate, accountable, and transparent actors and ideologies. Tech companies should have a seat at the table, but they cannot be allowed to restrict other stakeholders from participating in the norm-creation and institution-building processes.