THE CYCLES OF GLOBAL TELECOMMUNICATION CENSORSHIP AND SURVEILLANCE

JONATHON W. PENNEY*

ABSTRACT

Internet censorship and surveillance is on the rise globally and cyber-warfare increasing in scope and intensity. To help understand these new threats, commentators have grasped at historical analogies often with little regard for historical complexities or international perspective. Unfortunately, helpful new works on telecommunications history have focused primarily on U.S. history with little focus on international developments. There is thus a need for further internationally oriented investigation of telecommunications technologies, and their history. This essay attempts to help fill that void, drawing on case studies wherein global telecommunications technologies have been disrupted or censored – telegram censorship and surveillance, high frequency radio jamming, and direct broadcast satellite blocking. The case studies suggest remarkable regulatory patterns or cycles with insights for current censorship and privacy threats and challenges.

* The author would like to thank Joseph Nye, Jonathan Zittrain, Ron Deibert, Masashi Crete-Nishihata, Joss Wright, Harry Lewis, Dorothy Zineberg, Victoria Nash, Ariel Katz, Carys Craig, Jennifer Granick, Fred von Lohmann, Eric Goldman, Dan Hunter, Scott Boone, Kendra Albert, Ryan Budish, Andy Sellars, Molly Sauter, Phillipa Gill, Adam Holland, Amar Ashar, Dan Jones, Enrique Armijo, Lorne Sossin, François Tanguay-Renaud, and Simon Stern, for comments, questions, and feedback on earlier drafts and talks upon which this work is based. He would also like to thank participants for his talks at the 2013 Internet Law Work in Progress Conference, Santa Clara High Tech Law Institute, Santa Clara Law School, Santa Clara, California, March 16, 2013; Berkman Luncheon Series, Berkman Center for Internet & Society, Harvard University, February 26, 2013; Free and Open Communications on the Internet (FOCI) Workshop, 21st USENIX Security Symposium, Bellevue, WA; and participants at the 2014 University of Toronto-Osgoode Hall Law Junior Scholars Forum, April 25, 2014, Osgoode Hall Law School, Toronto, Ontario.

TABLE OF CONTENTS

1. INTRODUCTION

Internet censorship and surveillance is on the rise globally with state cyber-policing capabilities rapidly evolving and cyber warfare becoming a concern for major infrastructure and industries.[1] To help understand these new threats – and their implications for global telecommunications and relations – commentators have grasped at historical analogies, with Cold War parallels commonly raised, often with little context or regard for

---

[1] For a discussion of not only increasing international state censorship – including political and non-political filtering – but also broader notions of power and cyberwarfare, see Joseph S. Nye, Jr, *Cyber Power*, *in* JOSEPH S. NYE, JR., THE FUTURE OF POWER IN THE 21ST CENTURY (2011), *available at* http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf. For a discussion of how technology increases the scope and reach of state surveillance, and the implications of that reality, see JONATHAN L. ZITTRAIN, THE FUTURE OF THE INTERNET AND HOW TO STOP IT 109–23 (2008). In terms of reports of increasing surveillance, see Zach Miners, *Latest Transparency Reports Show Steady Rise in Surveillance Data Requests*, IDG NEWS SERV. (Mar. 2, 2014, 9:31 PM), http://news.idg.no/cw/art.cfm?id=C06C2F1A-E70F-545F-696A17DD7891B679; *Special Report on Internet Surveillance*, *Focusing on 5 Governments and 5 Companies "Enemies of the Internet,"* REPORTERS WITHOUT BORDERS, *available at* http://en.rsf.org/special-report-on-internet-11-03-2013,44197.html ("[G]overnments are increasingly using technology that monitors online activity . . ."); ONI Team, *Global Internet Filtering in 2012 at a* Glance, OPEN NET INITIATIVE (Apr. 3, 2012), http://opennet.net/blog/2012/04/global-internet-filtering-2012-glance (noting that at least a third of Internet users live in countries with substantive Internet blocking or censorship); James Ball, *Angry Birds and 'Leaky' Phone Apps Targeted by NSA and GCHQ for User Data*, THE GUARDIAN (Jan. 28, 2014, 2:51 AM), http://www.theguardian.com/world/2014/jan/27/nsa-gchq-smartphone-app-angry-birds-personal-data; David E. & Thom Shanker, *NSA Devises Radio Pathway into Computers*, N.Y. TIMES (Jan. 14, 2014), http://www.nytimes.com/2014/01/15/us/nsa-effort-pries-open-computers-not-connected-to-internet.html; Steven Rich & Barton Gellman, *NSA Seeks to Build Quantum Computer that Could Crack Most Types of Encryption*, WASH. POST (Jan. 2, 2014), http://www.washingtonpost.com/world/national-security/nsa-seeks-to-build-quantum-computer-that-could-crack-most-types-of-encryption/2014/01/02/8fff297e-7195-11e3-8def-a33011492df2story.html; Nicole Perlroth et al., *NSA Able to Foil Basic Safeguards of Privacy on Web*, N.Y. TIMES (Sept. 5, 2013), http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?_r=0. Finally, on the costs and risks of cyberwar for infrastructure and industry, see Julie Hull, Himanshu Khurana, Tom Markham & Kevin Staggs, Staying in Control: Cybersecurity and the Modern Electric Grid, 10 IEEE POWER & ENERGY MAG. 41, 41–48 (2012); *see also* Kenneth Geers, *Cyberspace and the Changing Nature of Warfare*, SC MAG., Aug. 27, 2008, http://www.scmagazineus.com/cyberspace-and-the-changing-nature-of-warfare/article/115929/.

consistency or historical complexities.[2]

Helpfully, there have been some more comprehensive works on telecommunications history produced in recent years,[3] but these have primarily explored U.S. history and industry, with less focus on international developments or case studies. For example, Richard R. John's *Network Nation: Inventing American Telecommunications*[4] provides an excellent account of both the

---

[2] Sean Lawson, *Putting the "War" in Cyberwar: Metaphor, Analogy, and Cybersecurity Discourse in the United States*, 17 FIRST MONDAY 1, 2 (2012), http://firstmonday.org/ojs/index.php/fm/article/view/3848/3270 ("[P]olicy-makers and military leaders have looked primarily to war-related historical analogies and metaphors to aid their understanding of and responses to cyber security challenges"). This includes Western media too – see, for example, Sanger & Shanker (2014), *supra* note 1 (comparing Chinese malware tracking to Soviets tracking submarines in the Cold War); Noah Schachtman & Peter W. Singer, *The Wrong War: The Insistence on Applying Cold War Metaphors to Cybersecurity Is Misplaced and Counterproductive*, BROOKINGS INST. (Aug. 15, 2011), *available at* http://www.brookings.edu/research/articles/2011/08/15-cybersecurity-singer-shachtman.

[3] *See e.g.*, Dwayne Winseck, *Review Essay: Network Nation: Inventing American Telecommunications*, 53 BUS. HIST. 641–47 (2011) (providing a review of RICHARD R. JOHN, NETWORK NATION: INVENTING AMERICAN TELECOMMUNICATIONS (2010)); TIM WU, THE MASTER SWITCH: THE RISE AND FALL OF INFORMATION EMPIRES (2010) (illustrating the history of cable, from the evolution of cable as a "dive bar[,] . . . attract[ing] shady characters" in the 1960s to the fight between broadcasting and cable, to "corporate reincarnation" and conglomeration of the film industry, broadcast networks, and cable companies in the 1980s and 1990s). *Id.* at 178–79, 205. There is additional scholarship that is less comprehensive – for example, focusing on a single technology or industry sector – but nevertheless, they provide insightful explorations. *See, e.g.*, ROBERT MACDOUGALL, THE PEOPLE'S NETWORK: THE POLITICAL ECONOMY OF THE TELEPHONE IN THE GILDED AGE (2014); DAVID HOCHFELDER, THE TELEGRAPH IN AMERICA, 1832–1920, 181 (2012) (providing a chronology of the telegraph in America); COMMUNICATIONS UNDER THE SEAS: THE EVOLVING CABLE NETWORK AND ITS IMPLICATIONS (Bernard Finn & Daqing Yang, eds., 2009) (focusing mainly on cable network evolution); Sumit K. Majumdar, Ulku Yaylacicegi & Rabih Moussawi, *Mergers and Synergy: Lessons from Contemporary Telecommunications History*, 36 TELECOMM. POL'Y 140, 154 (2012). For a focus on an Asian perspective, see DAQING YANG, TECHNOLOGY OF EMPIRE: TELECOMMUNICATIONS AND JAPANESE EXPANSION IN ASIA, 1883–1945 (2010).

Beyond mere telecommunications history, scholars like Yochai Benkler, Susan Crawford, and Brett Frischmann have offered important insights into factors driving regulatory and technological developments in telecommunications, such as licensing practices, infrastructure, or industry monopolies. *See, e.g.*, Yochai Benkler, *Open Wireless vs. Licensed Spectrum: Evidence from Market Adoption*, 26 HARV. J.L. & TECH. 69, 90–93 (2012); SUSAN CRAWFORD, CAPTIVE AUDIENCE: THE TELECOM INDUSTRY AND MONOPOLY POWER IN THE NEW GILDED AGE (2013); BRETT FRISCHMANN, INFRASTRUCTURE: THE SOCIAL VALUE OF SHARED RESOURCES (2012).

[4] Dwayne Winseck, *Review Essay: Network Nation: Inventing American Telecommunications*, 53 BUS. HIST. 641–47 (2011) (providing a review of RICHARD R. JOHN, NETWORK NATION: INVENTING AMERICAN TELECOMMUNICATIONS (2010)).

telegraph and telephone's rise and evolution with American telecommunications, yet the work fails to fully consider how these developments relate to similar global changes at the time.[5] Tim Wu also offers an insightful account of information industries in *The Master Switch: The Rise and Fall of Information Empires*.[6] However, Wu's eyes are trained toward current U.S. debates about network neutrality and telecommunications regulation, and thus focuses primarily on American history, leaving important questions open concerning the impact and role of international telecommunications history and regulatory trends.[7]

Given the international character of telecommunications technologies like the Internet, and the tendency for commentators to draw historical parallels, there is a need for further investigation of telecommunications technologies and their history, with an eye to international developments. Indeed, Ross Anderson, a leading technology researcher, has recently called for a more systematic and interdisciplinary approach to these issues, arguing, for example, that the dynamics of information industries has implications for how we understand and regulate international relations and conflict.[8] This essay attempts to offer some pieces to that puzzle, with an examination of case studies wherein global telecommunications technologies have been disrupted or censored – telegram censorship, surveillance, and cable cutting, high frequency radio jamming, and direct broadcast satellite blocking – and how the world community responded to that disruption through international law and politics. Drawing on that history, this essay aims to show first that case studies do suggest certain patterns or cycles of global telecommunications censorship and surveillance comparable to Wu's framework; but that these challenges are neither inevitable nor insurmountable. Rather, these

---

[5] *Id.*

[6] WU, *supra* note 3.

[7] *See* Jonathan D. Aronson, *Book Review: The Master Switch: The Rise and Fall of Information Empires*, 5 INT'L J. COMMC'NS 89, 93 (2011) (reviewing TIM WU, THE MASTER SWITCH: THE RISE AND FALL OF INFORMATION EMPIRES (2010)).

[8] Ross Anderson, *Privacy Versus Government Surveillance: Where Network Effects Meet Public Choice* 1, Proc. 13th Annual Workshop on the Economics of Information Security (WEIS 2014), *available at* http://weis2014.econinfosec.org/papers/Anderson-WEIS2014.pdf ("The forces that lead to pervasive monopolies in the information industries – network effects, technical lock-in and low marginal costs – are pervasive in the affairs of states too, once we look for them; they are just not yet recognised as such.").

patterns may be "broken" or mitigated by more cooperative international regulatory approaches. Along the way, the paper also draws on the case studies to offer guidance as to future trends in Internet regulation, censorship, and surveillance and lessons to tackle such challenges.

Beyond these bigger questions, the work's focus on international policy-making means it should also provide some insights on typical questions raised about Internet censorship and surveillance, and its resistance, under international law. For example, a few previous studies have examined or noted the legal implications of Internet filtering,[9] mapping,[10] or censorship circumvention,[11] yet none have examined, in depth, how circumvention of state-implemented Internet censorship or surveillance fits within international law and its politics. This is perhaps because the use, distribution, or development of Internet censorship and surveillance resistant systems or censorship circumvention tools – what will be referred to here as censorship or surveillance resistance activities – are often seen as the work of private citizens, organizations, and other non-state actors, and not subjects of the international system. Still, the legitimacy of such activities has been questioned as either Western interference with other states' sovereign values or as a threat to national security.[12] Situating such activities within broader international legal rules or norms can provide meaningful "moral, rhetorical, and at least

---

[9] OpenNet Initiative, *A Starting Point: Legal Implications of Internet Filtering* 1, 4, OPEN NET INITIATIVE (2004), http://opennet.net/docs/Legal_Implications.pdf.

[10] Joss Wright, Tulio de Souza & Ian Brown, *Fine-Grained Censorship Mapping: Information Sources, Legality and Ethics* 1, 1–3, 1st USENIX Workshop on Free and Open Commc'ns on the Internet (2011), *available at* http://static.usenix.org/events/foci11/tech/final_files/Wright.pdf.

[11] Derek Bambauer, *Cybersieves*, 59 DUKE L.J., 377, 441–43 (2009).

[12] *See e.g.*, Evgeny Morozov, *Freedom.gov*, FOREIGN POL'Y (Jan. 3, 2011), http://www.foreignpolicy.com/articles/2011/01/02/freedomgov?page=full (noting that Internet freedom is viewed in some quarters as "another Trojan horse for American imperialism"); Andrew Lloyd, *Increasing Global Demand for an Uncensored Internet – How the U.S. Can Help Defeat Online Censorship by Facilitating Private Action*, 41 VAND. J. TRANSNAT'L. L. 299, 300–01 (2008) (arguing that U.S. funding "anti-jamming" technologies to defeat censorship perceived as "imposing its own standards of decency and morals onto China and other countries . . ."); Philip J. Oliveri, *Technology Software that Counters Internet Jamming: Its Role in the U.S. and in Non-Democratic Countries*, SYRACUSE L. & TECH J. 5, 9 (2003) (suggesting that promoting anti-jamming and anti-circumvention tools infringes on state sovereignty); Jennifer Shyu, *Speak No Evil: Circumventing Chinese Censorship*, 45 SAN DIEGO L. REV. 211, 239–42 (2008–2009) (speaking of censorship circumvention and anonymizing tools as a threat to national security).

arguable legal support" to justify censorship or surveillance resistance and its various components like filter circumvention or anonymous access.[13]

International law, it is often assumed, has little to say about Internet censorship, and even less to offer in constraining or resisting it, because the practice involves two irreconcilable principles of international law – rights to information and expression and states' sovereign right to police their territories.[14] Yet this is likely an overly simplified account. Thus, examining case studies involving global communication disruption, and their legal and political dimensions, could offer insights into both regulatory patterns and lessons for similar challenges today.[15]

2. FRAMING THE INQUIRY

Wu's *Master Switch* introduces us to what he calls "the Cycle" within U.S. telecommunications industry, that is, the tendency for information empires to begin with a period of openness and novelty, but eventually progress toward monopoly, centralization, and a closed approach to telecommunications.[16] This essay certainly draws on Wu's research for guidance in outlining comparable developments, but unlike *Master Switch*, the patterns or cycles identified are internationally oriented, tracking a seeming pattern by which global telecommunications technologies are adopted, facilitated, controlled, and then censored or monitored at

---

[13] *See* Michael Froomkin, *Lessons Learned Too Well* 35 (Miami Law Research Paper Series, Paper No. 2011-29, 2011), *available at* http://ssrn.com/abstract=1930017.

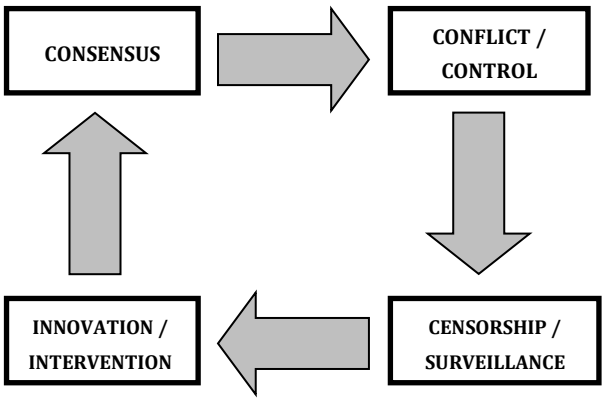
[14] Rochelle B. Price, *Jamming and the Law of International Communications*, 5 MICH. Y.B. INT'L LEGAL STUD., 391, 391–92 (1984); Katherine Tsai, *How to Create International Law: The Case of Internet Freedom in China*, 21 DUKE J. COMP. & INT'L L. 401, 402–03 n.402 (2011) (questioning whether international law has an answer to China's sovereign claim to censor Internet content).

[15] *See generally* Jonathan Zittrain & John Palfrey, *Reluctant Gatekeepers: Corporate Ethics on a Filtered Internet*, *in* ACCESS DENIED: THE PRACTICE AND POLICY OF GLOBAL INTERNET FILTERING 103–22 (Ronald Diebert et al. eds., 2008), *available at* http://access.opennet.net/wp-content/uploads/2011/12/accessdenied-chapter-5.pdf (discussing the complexities involved in these issues); Eszter Hargittai, *Radio's Lessons for the Internet*, 43 COMMC'NS OF THE ACM 51, 52 (2000) (asserting that a "historical look" can provide a clearer understanding of factors shaping the "media landscape").

[16] WU, *supra* note 3, at 6–7.

an international level (see **Figure 1.1**).

Figure 1.1
An Adaption of Wu's "Cycle"
in the Global Telecommunications Context?



Here, case studies focusing on three global telecommunications technology – telegraph, radio, satellite – were selected largely on the basis of the high level of international regulatory attention these technologies attracted. The International Telegraph Union (today the International Telecommunication Union), the world's central regulatory agency for international telecommunications, was founded to regulate telegraph communications and, in the 20th Century, its name change reflected a broader mandate to cover other technologies.[17] The ITU also organized large-scale regulatory efforts on radio and satellite in the Post-War period.[18]

---

[17] *Overview of ITU's History*, INT'L TELECOMM. UNION, *available at* http://www.itu.int/en/history/Pages/ITUsHistory.aspx (noting major initiatives on the telegraph, and, after the Second World War, both on radio as well as satellite). Additionally, a predominant number of the hundred odd ITU telecommunication conferences and assemblies held since its founding, have focused on the telegraph (24), radio (62), and space/satellite (6). In contrast, the ITU has held few on television (2) and has held none on "global" communication technologies like the GPS and telex. *See List of ITU Conferences, Assemblies and Events*, INT'L TELECOMM. UNION, *available at* http://www.itu.int/en/history/Pages/ListOfITUConferencesAssembliesAndEvents.aspx (delineating the conferences, assemblies, and events and showing that there have been only two conferences focused on the television in 1986 and 1989).

[18] Hargittai, *supra* note 15.

As will be seen, the case studies suggest that global telecommunications technologies also appear to follow comparable patterns to Wu's "Cycle." The technologies are first adopted or promoted in an initial stage, where the international community, and most states, develops a consensus about the technology's advantages and positive potential. This consensus typically becomes reflected in law and policy at the time. However, as states begin to fully understand the technology – both as a potential tool to promote national interests abroad, and as a threat to the state's agenda or security – that consensus breaks down. This leads to a sustained period of conflict, often taking the form of information conflicts or information wars, and a bid by governments to attempt to control the technology, both domestically and through international efforts. Such "control" typically manifests itself in both censorship and surveillance of the technology in question. What appears to disrupt (or reset) the "pattern" is typically technological innovation or regulatory intervention. For example, a new communications technology eclipses the old, or there is some kind of regulatory intervention by international entities that pushes things in a different direction.

These regulatory patterns and the above-noted framework should be kept in mind as the case studies are explored. Importantly, however, unlike Wu, whose capitalization of his "Cycle" suggests the process he analyzes is inevitable, the patterns explored in these case studies are not treated as either essential or inevitable, nor should they be. There are certainly other technologies (like global positioning systems (GPS)) that are arguably "global" and relating to communications that do not follow these patterns of international conflict, regulation, surveillance, and control. Moreover, drawing on various aspects of the case studies, this paper also argues that the very patterns observed may be mitigated, even "broken," by more cooperative international regulatory efforts. These case studies will also hopefully offer insights for comparable contemporary technologies, namely, the Internet.

3. GLOBAL TELECOMMUNICATIONS CONTROL: THREE CASE STUDIES

3.1. Case Study One: Telegraph Cable Cutting, Censorship, and Surveillance

Internet censorship is often compared to Cold War radio jamming,[19] but the telegraph offers our first case study. In fact, one of the earliest instances where transnational communications were disrupted by states involved the telegraph – submarine cable cutting and cable message surveillance and suppression in the late 19th and early 20th century. The first transatlantic submarine cables, through which telegraph cables could be communicated, were laid by the 1850s, only a few years after the introduction of telegraph.[20] Through efforts led mainly by Britain, an extensive web of submarine cables were subsequently laid between countries in Europe, Africa, and Asia, and by the 20th century most of the world was linked, establishing one of the earliest global telecommunications networks.[21] British companies, with the assistance of the Empire, owned and controlled the vast majority of this submarine cable network.[22] The submarine telegraph cable network proved a powerful tool. Its global reach for commerce, diplomacy, and the free flow of information it promoted, allowed rapid, safer, and more secure communications between governments, dissemination of information between populations, and more efficient coordination for world shipping and trade.[23]

Much like Internet censorship today, the submarine cable

---

[19] *See, e.g.*, Hargittai, *supra* note 15, at 51 (comparing the origins and subsequent regulation of radio communication with Internet censorship).

[20] *See generally* DANIEL R. HEADRICK, THE INVISIBLE WEAPON: TELECOMMUNICATIONS AND INTERNATIONAL POLITICS: 1851–1945, 28–49 (1991) (providing a historical review of the development of telegraph cables, including the first transatlantic submarine cables and the expansion of the global cable network between 1866–1895).

[21] *Id.; see also* A. Pearce Higgins, *Submarine Cables and International Law,* 2 BRIT. Y.B. INT'L L. 27, 27–30 (1922) (emphasizing the international importance of the cables and noting that the Treaty of Versailles lists the cables, "as follows: Emden-New York, Teneriffe Monrovia, . . . Constantinople-Constanza"). *Id.* at 27.

[22] Higgins, *supra* note 21, at 28 ("The British public had early grasped the importance of the cable as a means of linking up the world-wide Empire . . ."); UNITED NATIONS ENV'T PROGRAM (UNEP), SUBMARINE CABLES AND THE OCEANS: CONNECTING THE WORLD 13 (2009) [hereinafter UNEP], *available at* http://www.iscpc.org/publications/ICPC-UNEP_Report.pdf.

[23] UNEP, *supra* note 22, at 13, 26.

network's importance to global communications also made it a target for disruption by hostile states that, strategically, could isolate or weaken enemies by disrupting state and commercial communications. And while submarine cables were much more secure than land cables, they could be damaged, and with the right equipment, cut.[24] Early on, the telegraph cable network was mostly seen as beneficial to trade, commerce, and diplomacy.[25] Thus, the telegraph's international cable network was mostly developed through private investment – companies seeking to benefit commercially from this new communications technology.[26] Yet, with the use of telegraph cables by the British Army during the Crimean War and, most importantly, a cable link to India – a key regional asset in the Empire – the British Government did not take long to realize the strategic importance of the telegraph network and its vulnerability to cable-cutting and other disruptions by hostile States.[27] The telegraph cable network was also vulnerable to censorship and surveillance. Most of the global network was controlled by public and private companies from a handful of States – with Britain being the most dominant, though Germany had also invested heavily.[28] If either State decided to block or suppress telegraph communications, they would be well positioned to do so.[29]

---

[24] P.M. Kennedy, *Imperial Cable Communications and Strategy, 1870–1914*, 86 ENGLISH HIST. REV. 728 (1921).

[25] *Id*. at 729.

[26] *Id*.

[27] *Id*. at 732.

[28] Higgins, *supra* note 21, at 27–30.

[29] Britain would quickly take advantage of its strategic position at the eve of World War I. *See* Kennedy, *supra* note 24, at 751–52 ("On the other hand, the Admiralty showed extraordinary speed in cutting the German cables: on the morning after the British ultimatum to Berlin had expired, for example, the two ends of the German Atlantic cable had been cut and were later taken into the harbours of Falmouth and Halifax. Other lines were similarly dealt with, and the German cables, like their colonies, were divided amongst the victorious allies in the Versailles settlement. Moreover, the political advantages which Britain (and to a lesser extent, France) gained from the virtual control of war news to the United States and to the rest of the neutral world confirmed the value of this system of communication.") (footnotes omitted).

3.1.1. Consensus: Facilitating and Protecting Telegraph Communications and the Telegraph Cable Network

Not surprising given its obvious importance to global communications and commerce at this time, Britain worked to build international consensus about the need to promote the telegraph telecommunications network. This was not difficult, at least at this time. As noted by historian P.M. Kennedy, to the "mid Victorian mind," the telegraph and its cable communications network was mostly viewed as one of a "long series of technological innovations" that would mainly contribute to "trade and prosperity," with "businessmen, journalists, and diplomats" as the chief beneficiaries.[30] Moreover, a "cable boom" that began in the 1860s and peaked in the 1870s – spurred on largely through private commercial efforts – meant that by this time much of Europe, and parts of both the Middle East and Asia, were connected by land and submarine telegraph cables making the telegraph communications valuable to a number of powers like Russia, France, Germany, and the United States.[31]

The goodwill felt internationally toward the telegraph cable network – despite being largely owned by British private interests – is reflected in correspondence between U.S. President James Buchanan and Queen Victoria in 1858, on the occasion of the first transatlantic cable being sent.[32] The Queen had written to the President about the submarine cable, proclaiming it would provide an "additional link between the nations, whose friendship is founded upon their common interest and reciprocal esteem[;]"[33] to which the President replied:

> May the Atlantic telegraph, under the blessing of heaven, prove to be a bond of perpetual peace and friendship between the kindred nations, and an instrument destined by Divine Providence to diffuse religion, liberty, and law

---

30 Kennedy, *supra* note 24, at 729.

31 HEADRICK, *supra* note 20, at 93; Kennedy, *supra* note 24, at 732–37.

32 Kennedy, *supra* note 24, at 729.

33 LORDS OF THE COMM. OF PRIVY COUNCIL FOR TRADE & THE ATLANTIC TEL. CO., REPORT OF THE JOINT COMMITTEE TO INQUIRE INTO THE CONSTRUCTION OF SUBMARINE TELEGRAPH CABLES; TOGETHER WITH THE MINUTES OF EVIDENCE AND APPENDIX 232 (1861).

> throughout the world. In this view will not all the nations of Christendom spontaneously unite in the declaration that it shall be forever neutral, and that its communication shall be held sacred in passing to the place of their destination, even in the midst of hostilities?[34]

Similar sentiments can also be seen years later in W.H. Russell's *The Atlantic Telegraph*, his official account of the 1865 expedition to lay the "Great Eastern" cable across the Atlantic Ocean. Russell wrote of the Cable of 1865 as an "enduring link, which, under God's blessing, may confer unnumbered blessings on the nations which the ocean has so long divided" and the "greatest work of civilized man, and the grandest exposition of the development of the faculties bestowed on him to overcome material difficulties. . . ."[35]

An expression of the times, it is not surprising similarly positive sentiments would be reflected in the more significant international legal measures enacted during this time concerning global telegraph communications: the International Telegraph Convention (first enacted in 1865, but substantially altered in 1872 and 1875) and the 1884 International Convention for the Protection of Submarine Cables.[36] The global consensus and positive attitude about the telegraph particularly permeated the 1875 international telegraph conference in St. Petersburg that led to the 1875 Convention, where "friendly relations" and diplomacy among world powers were pervasive.[37] The 1875 Telegraph Convention

---

[34] Kennedy, *supra* note 24, at 730 (citation omitted) (quoting President Buchanan in his response to Queen Victoria's greetings). *See also* W.H. RUSSELL, THE ATLANTIC TELEGRAPH (1865) (chronicling the engineering process as well as the cultural significance of laying the transatlantic cable, thereby connecting Europe with the New World).

[35] RUSSELL, *supra* note 34, at 103–04.

[36] The 1875 International Telegraph Convention is often referred to as the "St. Petersburg Convention," after the location of the conference. The Submarine Convention was signed in 1884 but did not come into effect until 1888. *See* Ted Magder, *The Origins of International Agreements and Global Media: The Post, the Telegraph, and Wireless Communication Before World War I*, *in* THE HANDBOOK OF GLOBAL MEDIA AND COMMUNICATION POLICY 23, 30–33 (Robin Mansell & Marc Raboy eds., 2011) (describing the evolving political context in which the St. Petersburg Convention was negotiated).

[37] J. Henry Glazer, *The Law-Making Treaties of the International Telecommunication Union Through Time and in Space*, 60 MICH. L. REV. 269, 269–70 (1962).

would turn out to be the most significant international legal instrument concerning communications in this era.[38]

These measures codified previous treaties and customary international law but also included innovations; as we will see, the measures proved effective in protecting the telegraph cable network, at least in times of peace. The 1875 International Telegraph Convention (enacted with annexed Service Regulations to help govern operations), declared that "all persons" have a "right" to communicate by "international telegraph" and required states to "adopt all necessary measures to ensure the secrecy and prompt despatch of [telegraph correspondences]."[39] These rights and protections – and others in the 1875 Telegraph Convention – drew upon similar provisions in earlier Conventions. Indeed, the 1871 Telegraph Convention, a product of the 1871–1872 Rome Conference, similarly recognized a "right of all persons to correspond by means of the International Telegraphs" (Article 4) and that signatory states would "undertake to adopt all necessary measures to insure the secrecy of messages, and their prompt despatch" (Article 5).[40] The 1875 Telegraph Convention was meant to codify these articles as more "permanent" or "fundamental"; a reflection of the prior "decade of experience."[41]

Such expansive language was quite innovative for international legal measures at that time. The traditional understanding in international law – both in the 19th Century right through most of the 20th – was that individuals were not the subjects of international law, only states, and that individuals themselves existed only at the "utmost periphery" of international legal

---

[38] HEADRICK, *supra* note 20, at 13 ("The most important conference was the one held in St. Petersburg in 1875.").

[39] International Telegraph Convention art. II, July 22, 1875, 148 C.T.S. 416, *available at* http://www.itu.int/dms_pub/itu-s/oth/02/01/S02010000044002PDFF.pdf. *See International Telegraph Convention*, 7 AM. J. INT'L. L. 276 (Supp. 1913); FRANCIS LYALL, INTERNATIONAL COMMUNICATIONS: THE INTERNATIONAL TELECOMMUNICATION UNION AND UNIVERSAL POSTAL 32–35 (2011) (reprinting the Convention in English).

[40] International Telegraph Convention arts. IV, V, Jan. 14, 1872, 143 C.T.S. 415, *available at* http://www.itu.int/en/history/Pages/PlenipotentiaryConferences.aspx?conf=3&dms=S0201000003.

[41] LYALL, *supra* note 39, at 33; HEADRICK, *supra* note 20, at 13 ("The most important [telegraph] conference was the one held in St. Petersburg in 1875. Its convention codified the experience of the previous decade, including some important political decisions.").

thinking.[42] Thus, to have international legal documents in the 1870s with such broad support bestowing "all persons" with a communication "right" with respect to the international telegraph network was a unique and innovative idea, arguably foreshadowing broader shifts in international law that would not come until a century later.

Yet, beyond this recognition of individual rights, State interests were nevertheless essential to the telegraph network's operation and protection. Indeed, some commentators have read these provisions more narrowly; arguing that notwithstanding this lofty language, the Convention ensured national security was paramount because it reserved to States the right to stop transmission of any "private telegram" if not doing so was "dangerous" to the security of the State or contrary to order or morality.[43]

However, that is not an entirely accurate reading because it ignores how the Convention operated in practice – with provisions on notice and the settling of accounts when telegrams are delayed or suspended, in both its Articles and annexed Service Regulations. Government "censorship" of both private and state telegrams sent through the international telegraph system was explicitly dealt with in the 1875 Telegraph Convention – in Articles 7 and 8. Such telegraph censorship involved what we would today consider state and state-sanctioned surveillance – government or military officials employed by telegraph companies and operators to monitor, suppress, and confiscate, for state purposes, "suspicious" cable

---

[42] Andreas Muller, *Review: The Individual in the International Legal System: Continuity and Change in International Law*, 23 EUR. J. INT'L L. 275, 275 (2012) (providing a review on KATE PARLETT, THE INDIVIDUAL IN THE INTERNATIONAL LEGAL SYSTEM: CONTINUITY AND CHANGE IN INTERNATIONAL LAW (2010)) ("Whether and where to locate the individual in the universe of international law has become a standard question for the discipline. While in the 19th and still in the early 20th centuries international legal doctrine could not see in the human person anything other than a mere object of international law, at the beginning of the 21st century, the individual presents itself as *habitué* of international law with major treatises dedicating a substantial number of pages, if not whole chapters to the topic. The last hundred years have thus witnessed a remarkable development which has shifted the individual's place in international law from the utmost periphery of the discipline to perhaps not its centre, but at least to its inner circles.") (footnotes omitted). *See generally* Ole Spiermann, *Twentieth Century Internationalism in Law*, 18 EUR. J. INT'L L. 785 (2008).

[43] *See, e.g.*, Magder, *supra* note 36, at 31–32 (highlighting that articles 6 and 7 make clear that national security takes priority over the "right of communication.").

messages.[44] Article 7 is the central Convention provision dealing with telegraph censorship, which was limited to "private" telegrams:

"The high contracting parties reserve to themselves the right to stop the transmission of any private telegram which may appear dangerous to the security of the State, or which may be contrary to the laws of the country, to public order, or decency."[45]

Similarly, Article 8 of the Convention conferred on signatory states the power to "suspend" the international telegraph service itself, more "generally" or certain "lines" for "any length of time."[46] Again, the right to "stop" telegrams (under Article 7) or "suspension" (under Article 8) provides states with an opportunity for surveillance, delay, and confiscation of any "suspicious" cables or telegrams being sent through the service.[47] For state censors, these are some powerful tools to censor and survey telegraph communications.

Yet, these "censorship" Articles were subject both to notice requirements and notifications via account settlement and reimbursement. Explicit notice requirements for Article 8 are codified directly in its text:

"Each government also reserves to itself the right to suspend the international telegraph service for an indefinite period, if it deem necessary; either generally or only upon certain lines and for certain classes of correspondence, upon condition that it immediately advises each of the other Contracting Governments."[48]

---

[44] Jill Hills, *What's New? War, Censorship, and Global Transmission*, 68 INT'L COMMC'N GAZETTE 195, 197–98 (2006) (describing the appointment of "ex-military men" to work as "censors" at telegraph company stations who, with "knowledge of foreign languages" monitor cable messages sent through the company waystations and "delay" or confiscate "suspicious" messages, and relay said messages to the Chief Censor in London).

[45] International Telegraph Convention, *supra* note 39, art. VII. The original French text of Article 7 is as follows: "Les Hautes Parties contractantes se réservent la faculté d'arrêter la transmission de tout télégramme privé qui paraîtrait dangereux pour la sécurité de L'Etat ou qui serait contraire aux lois du pays, à l'ordre public ou aux bonnes moeurs."

[46] *Id*. art. VIII.

[47] *Id.* arts. VII, VIII.

[48] International Telegraph Convention (1875), art. VIII, *available at* http://www.itu.int/dms_pub/itu-s/oth/02/01/S02010000094002PDFE.pdf (emphasis added). The original French text of Article 8 is as follows:

> Chaque Gouvernement se réserve aussi la faculté de suspendre le service de la télégraphie internationale pour un temps indéterminé, s'il le juge

Therefore, notice must be sent to *all* other states if a state chooses to "suspend" telegraph communications for whatever reason. Similarly, states exercising the right to "stop" private or non-state telegrams under Article 7 were required under (then) Service Regulation XL to "immediately" notify the "Administration," that is, the authority responsible for regulating and administrating the telegraph system in a given state:

> The power reserved under Article 7 of the Convention of stopping the transmission of any private telegram which may appear dangerous to the security of the State, or which may be contrary to the laws of the country, to public order or decency, should only be made use of, on condition of immediately advising the Administration to which the original sending office belongs.[49]

As Hills has noted, the widespread interpretation of the Regulation, or "normal practice," was for the telegraph administrative authority "to inform the sender of the telegram,"[50]

> nécessaire, soit d'une manière générale, soit seulement sur certaines lignes et pour certaines natures de correspondances, à charge par lui d'en aviser immédiatement chacun des autres Gouvernements contractants.

[49] International Telegraph Convention (1875), Service Regulation XL (English trans.), *available at* http://www.itu.int/dms_pub/itu-s/oth/02/01/S02010000044002PDFF.pdf (emphasis added). The official printing of this version of the Regulation was issued in French:

> Il ne doit être fait usage de la faculté réservée à l'article 7 de la Convention, d'arrêter la transmission de tout télégramme privé qui paraîtrait dangereux pour la sécurité de l'Etat, ou qui serait contraire aux lois du pays, à l'ordre public ou aux bonnes moeurs qu'à charge d'en avertir immédiatement l'Administration de laquelle dépend le bureau d'origine.

[50] Hills, *supra* note 44, at 197. This normal practice is also confirmed by comments in conference documents for the 1903 telegraph administrative conference. In providing "observations" on a proposed change to Regulation XLVI (by 1903, Regulation XL had been re-numbered to XLVI due to subsequent amendments to Regulations in other administrative conferences, and its 1903 version would be re-numbered again as XLV), the French delegation stated that "[p]ratiquement, le bureau d'origine est informé directement," that is, "[p]ractically, the office of origin is informed directly." In other words, the office in which the sender sent a telegram was informed of an Article 7 stoppage or interruption. Documents of the International Telegraph Conference of London, 326 (1903), *available at* http://www.itu.int/dms_pub/itu-s/oth/02/01/S02010000094802PDFF.pdf. Hills, it should be noted, refers to the

and in fact, the language of Regulation XL would be later amended to reflect that reality.[51] Any secretive and systematic telegram censorship and surveillance would obviously be undermined by these notice requirements. Even if the normal practice was not necessarily to inform the sender, the *risk* of such notice being given – by a state telegraph authority – would be a serious problem for any covert surveillance program monitoring state espionage or other "threats," because it could compromise its operations by disclosing its investigatory targets.

In fact, there is a good reason why the "normal practice" was for telegraph administrative authorities to notify the sender: because senders would receive notice anyway by virtue of Convention Regulations "refund" provisions. To promote the use of the telegraph system among the states, the International Telegraph Convention has important guarantees for transparent and fair accounting, including requirements for uniformity of charges for messages sent through the system (Article 10) and for states to "reciprocally . . . account" for any charges collected (Article 12).[52] Similarly, when the telegraph fails to deliver telegrams, senders can be refunded. Thus, when a state interferes with telegraph communications under Articles 7 or 8, Service Regulation LXX required the state to provide a refund:

"When a telegram is stopped under Articles 7 and 8 of the Convention, the charge made for its transmission is returned to the sender and the refund is supported by the Administration which stopped the telegram."[53]

---

later version of the 1903 version of Regulations. As will be seen, one of the exceptions she discusses (avoiding notice for Article 8 suspensions when "dangerous" for security) would not be added until 1903, years after the all-important 1875 conference, as tensions escalated before the First World War.

[51] In 1903, Germany proposed an amendment to the Regulation that would extend its Article 7 telegram stoppage notice requirements to include stoppages or interruptions of a telegram under Article 8. France, supporting Germany's proposal, also recommended changing the language of the Regulation to reflect the normal practice of states established by this time, which was to inform the sender by sending notice directly to the telegram's office of origin (the French delegation stated, "[p]ratiquement, le bureau d'origine est informé directement" or, in English, "[p]ractically, the office of origin is informed directly"). Both amendments were successful. *See generally* Documents of the International Telegraph Conference of London (1903), *supra* note 50, at 326.

[52] International Telegraph Convention (1875), *supra* note 39, art. X, XII (English trans.).

[53] International Telegraph Convention (1875), *supra* note 39, at Service Regulation LXX (English trans.). The official printing of this version of the

In other words, if a state censor stopped a telegram, then the sender would ultimately receive notice of that stoppage when he or she received a refund. Again, such notice by individual refund would frustrate the whole strategic purpose of secret telegraph surveillance by "tipping off" senders that they were being secretly monitored.

Together, these international legal measures effectively curtailed telegram communication censorship and surveillance operations. Britain, for example, took steps to secretly establish an elaborate "censorship" system of telegram surveillance and blocking through its predominant control over key telegraph infrastructure; but by the 1890s, British officials questioned the system's legality under the 1875 Telegraph Convention and reigned in operations.[54] The weakest guarantee in the broader protective scheme was Article 8, which allowed states to stop entire classes of telegram correspondence (e.g., any private telegram that dealt with military goods). Nevertheless, as of 1875, the Convention required general notice to all other contracting states on notice, and notice via refund for stoppage.

3.1.2. Promoting Secrecy in Communications

The 1875 Telegraph Convention promoted, and provided some important guarantees, for the use of secret codes and languages in telegrams communications. These provisions were arguably precursors to more modern forms of "rights" to use encryption for secrecy and privacy. The Convention not only recognized the aforementioned responsibility for states to "make all necessary provisions to [e]nsure the secrecy and quick dispatch" of telegraph communications, but also an express right to send private telegrams in "secret" code or language.[55]

Interestingly, this right was also protected through a mandatory non-discrimination communication policy, an early notion of "network neutrality" at least concerning secret telegrams. That is, where a state did not (under national law) allow telegrams

---

Regulation was issued in French: "La taxe d'un télégramme arrêté en vertu des articles 7 et 8 de la Convention est remboursée à l'expéditeur et le remboursement est à la charge de l'Administration qui arrêté le télégramme."

[54] Hills, *supra* note 44.

[55] International Telegraph Convention (1875), *supra* note 39, art. VI.

to be sent in secret language or code, they were not to treat such communications any differently, like stopping telegrams written in secret code or "suspending" telegraph service to prevent their passage. Rather, states were expressly obliged to allow any such secretly coded telegraph transmissions through their territory subject only to Article 8 suspension of services. This meant that if states did not allow secretly coded messages, they had to notify all contracting states.[56] In fact, different notions of neutrality in the broader telegraph network – like the uniform and neutral treatment of telecommunications traffic and charges – was a broader principle of the International Telegraph Convention, with Article 10 requiring the "charge for all messages exchanged, by the same route" be "uniform."[57] These Convention provisions, and the principles and aims underlying them, prevented states, at least without notice, from discriminating against "encrypted" or secretly encoded telegrams.[58]

Despite often-rudimentary ciphers, codes, and "cryptographic" methods, these provisions were also effective in preserving secrecy and privacy in telegram communications. Though codes and ciphers had been used in Europe since 1865, they proliferated among private enterprise after the 1875 Telegraph Convention, whose allowance for up to ten letters per "artificial" word eventually led to a "surge" in code making.[59] Since international telegrams had to be routed through numerous international cable way stations and thus handled by a number of people, companies

---

[56] International Telegraph Convention (1875), *supra* note 39, arts. VI, VIII.

[57] International Telegraph Convention (1875), *supra* note 39, art. X. The original French text of Article 10 is as follows:

> Les Hautes Parties contractantes déclarent adopter, pour la formation des Tarifs internationaux, les bases ci-après:
>
> La taxe applicable à toutes les correspondances échangées, par la même voie, entre les bureaux de deux quelconques des Etats contractants sera uniforme. Un même Etat pourra toutefois, en Europe, être subdivisé, pour l'application de la taxe uniforme, en deux grandes divisions territoriales au plus.

[58] Hills, *supra* note 44, at 197.

[59] Albeit after some regulatory wrangling and strong push back against restrictions by private codemakers. *See* HEADRICK, *supra* note 20, at 45 ("In 1890 the Paris ITU conference decreed that an official ITU codebook would be written to replace all private codes. Its publication in 1894 aroused such protests that the ITU had to back down and authorize existing codebooks. Finally in 1903 the IUT surrendered to the private code makers and allowed artificial words of up to ten letters. The result was a surge in code making . . . .").

desired privacy and secrecy for confidential or strategic corporate communications through codes and ciphers. As such, widespread use was driven by privacy and secrecy, but also economic factors: long distance telegrams had "astronomical" costs to send, and codes and ciphers reduced costs by replacing lengthier words with shorter artificial words or symbols.[60] Widespread use of both secret and standardized codes and ciphers rendered the "economics" of telegraph censorship and surveillance pricey. Indeed, while states had capabilities to monitor telegram communications and, later, "break" secret codes, languages, and ciphers, their proliferation posed a significant problem for mass surveillance. Code breaking was costly and time consuming, and as a result, state "censors" were very likely forced to focus on "specific targets."[61]

Beyond surveillance, cable-cutting legal measures were also taken. The Submarine Cables Convention was similarly effective in protecting the physical infrastructure of the telegraph network. It deterred cable cutting with a range of prohibitions and requirements, including requiring states to compensate owners for damage done to cables.[62] But again, this convention failed to address cable cutting among belligerent or warring states.

3.1.3. From Consensus to Conflict and Control: Censorship and Surveillance

Despite success, these international measures' failure to

---

[60] HEADRICK, *supra* note 20, at 45.

[61] Hills, *supra* note 44, at 201 (describing how the mass of messages that they encountered forced focusing on specific targets); CHARLES M. DOLLAR & JOAN R. GUNDERSON, AMERICA, CHANGING TIMES 853 (2d ed. 1982) (*"Much of this work of deciphering messages (1914–1918) was laborious and time consuming, still based largely upon frequency analysis. . ."*); DAVID PAULL NICKLES, UNDER THE WIRE: HOW THE TELEGRAPH CHANGED DIPLOMACY 181 (2003) (discussing a story whereby the U.S. State Department officials found it time consuming and difficult to decode their own coded cables).

[62] Hans Kelsen, *Collective and Individual Responsibility in International Law with Particular Regard to the Punishment of War Criminals*, 31 CALIF. L. REV. 530, 537–38 (1943) (discussing the provisions of the International Convention for the Protection of Submarine Telegraph Cables, including its provisions in article II providing for orders of "reparation" for damage done to cables by those responsible for "'[t]he breaking or injury of a submarine cable . . .'").

properly address censorship, surveillance, and cable cutting during war was a major oversight. This became a crucial flaw, once countries, namely Britain, started to understand how the global submarine cable network – most of which Britain owned or controlled – could be used to its national security and commercial advantage. And while the international legal framework governing telegraph telecommunications tied Britain's hands during peacetime; war, it would turn out, was another story.

As earlier noted, telegraph cable network was initially seen as mostly beneficial to trade, commerce, and diplomacy rather than strategically.[63] Yet, Britain was becoming increasingly aware of the telegraph system's strategic and military value, particularly in light of the role of censorship and cable cutting in the Spanish-American and Boer Wars.[64] In the Boer War, Britain installed military censors in Aden and Durban cable way stations, among others, and pursuant to Article 8 of the International Telegraph System, notified all other "contracting" states that it would be blocking all government "code" and "ciphered" telegrams from these cable stations linking Europe to South Africa.[65] This "blatant interference with non-military traffic" caused considerable backlash, with governments like Germany and France questioning the legality of the British actions and requests for compensation from commercial enterprises flooding into the British telegraph administration.[66]

These protests and requests for compensation ultimately forced the British Government to scale back the censorship, but a secret report by the British War Office concluded the censorship was a "success."[67] So, by 1900, British officials were "convinced" of both the value of telegraph "censorship" (and surveillance of cables to censor in practice) and – given the "futility" of existing "cipher" – the need for stronger cryptanalysis infrastructure.[68] Yet, to be

---

63 Kennedy, *supra* note 24, at 729 (noting how the submarine cable was created as a means to contribute to the growth of trade and prosperity).

64 *Id*.; *see also* Hills, *supra* note 44, at 199 (describing how the British government realized they could use the lines to censor commercial and financial transactions intended for the benefit of the enemy).

65 HEADRICK, *supra* note 20, at 88; Hills, *supra* note 44, at 199.

66 Hills, *supra* note 44, at 199; HEADRICK, *supra* note 20, at 88.

67 HEADRICK, *supra* note 20, at 88–89 (stating that the War Office felt that the mere fact that the censorship existed was a success); Hills, *supra* note 44, at 199.

68 Nicholas Hiley, *The Strategic Origins of Room 40*, 2 INTELLIGENCE & NAT'L SEC. 245, 249 (1987); HEADRICK, *supra* note 20, at 63–66, 83–84.

clear, the War Office report noted that the "success" of the Boer War telegraph censorship and surveillance was not so much because military censors obtained foreign intelligence by confiscating telegrams, but simply because the Article 8 notice deterred any foreign interests from even sending strategically important telegrams.[69] To ensure more effective, efficient, and secretive operations, changes to the international legal regime – defined primarily by the 1875 International Telegraph Convention – would need to be secured.

Yet, this would not be a simple task. Other world powers like France, Germany, and Russia, were jarred to reality by the way in which Britain had put its control over large portions of the global telegraph cable infrastructure to great strategic and military advantage during the war, despite being widely disruptive of communications among other neutral states.[70] This was an important turning point in the fate of the international telegraph system. It would first lead to a second cable laying "boom" as powers like Germany and France embarked on their own cable laying programs to "break" the British cable network monopoly.[71] It would also lead to an important clash at the subsequent international telegraph administrative conferences, as these powers worked to amend the Service Regulations – important to the operation of the 1875 International Telegraph Convention – to their advantage.

One key difference between the 1875 Telegraph Convention and earlier permutations like the 1872 Rome Revision, was that it was much shorter (only a few pages long), codifying the central articles of the Convention in more simplified language and relegating more complex provisions concerning the operation of the articles to the Service Regulations.[72] The idea was that the 1875 Telegraph Convention would codify these articles as more "permanent" or "fundamental,"[73] though the explicit text of the

---

[69] HEADRICK, *supra* note 20, at 88–89.

[70] Kennedy, *supra* note 24, at 748 (describing how the actions by the British spurred new cable construction by countries such as France and the United States).

[71] Kennedy, *supra* note 24, at 748; HEADRICK, *supra* note 20, at 111 (describing how the actions by the British caused a cable rivalry).

[72] LYALL, *supra* note 39, at 32.

[73] LYALL, *supra* note 39, at 33; HEADRICK, *supra* note 20, at 13 ("The most important [telegraph] conference was the one held in St. Petersburg in 1875. Its convention codified the experience of the previous decade, including some

Convention, under Articles 13 and 15, indicated that the Service Regulations "completed" the Convention and were of the same value as the Convention itself.[74] Nevertheless, the 1875 Convention would only be amended in larger diplomatic conferences while the supposedly less important Service Regulations could be changed in the smaller and more frequently held administrative conferences.[75] On one level, this strategy "worked," as the 1875 version of the International Telegraph Convention would not be changed for decades – not until 1932.[76] On another level, as we will see, easier revision of the Service Regulations would ultimately mean the undoing of much of these key Telegraph Convention protections against mass telegram censorship, surveillance, and control.

The very next International Telegraph Administrative Conference, held in London in 1903, would prove consequential. Germany, France, Great Britain, Russia, and several other state delegations to the conference, would clash bitterly over changes proposed to the earlier discussed Service Regulation XL (now "XLVI," re-numbered due to changes to regulations in earlier years). This Regulation, as noted, required that any stoppage of telegrams under Article 7 – for reasons of national security, legality, or public order or decency – required "immediate" notice to the state telegraph authority of the sending office with "normal" state practice under this requirement being "to inform the sender of the telegram."[77] This Regulation, in effect, guarded against covert telegram surveillance and stoppage because such practices would be disclosed or compromised by notice to senders.

Germany proposed extending these important individualized notice requirements to stoppages under Article 8, with France strongly supporting the amendment in debates about its

important political decisions.").

74 International Telegraph Convention (1875), *supra* note 39, art. XIII, XV.

75 LYALL, *supra* note 39, at 33.

76 HEADRICK, *supra* note 20, at 14 ("St. Petersburg was the last diplomatic conference on telegraph matters until 1932. After it came a series of administrative conferences attended by representatives of the various telegraph administrations during the following years: 1879, 1885, 1890, 1903, 1908, 1925, and 1928 . . ."); LYALL, *supra* note 39, at 32–33.

77 Hills, *supra* note 44, at 197. This normal practice is also confirmed by comments of the French delegation to the 1903 conference in stating that "[p]ratiquement, le bureau d'origine est informé directement," or, that in practice, the office of origin is informed directly. Documents of the International Telegraph Conference (1903), *supra* note 50.

ratification.[78] Their aim was likely to curtail future Article 8 abuses like the broad telegram disruptions employed by Britain during the Boer War under the authority of Article 8. Not surprisingly, Britain and Russia raised the strongest opposition to the amendment, with Japan and British India voicing concerns, while Hungary, Turkey, and Netherlands proposed compromises.[79] Britain and Russia shared similar concerns, stating such notice requirements for Article would be too onerous, or dangerous as notice would tip off targets of the stoppages, or that notice may disclose existing censorship operations.[80] Eventually, after prompting from Turkey, Netherlands, and Hungary to accommodate Britain and Russia's concerns about security, Germany offered a compromise: notice would be mandatory for Article 8 stoppages *except where it would appear dangerous to the security of the State* ("[s]auf les cas où il paraîtrait dangereux pour la sécurité de l'Etat").[81]

This compromise proposal to amend the Service Regulation notice requirements for Article 8 was accepted and ratified as the last act of the 1903 International Telegraph Conference. Unfortunately, it would utterly undermine the Convention's protections against large-scale telegraph censorship. Shortly after the Conference in 1904, the British War Office prepared a memo entitled "Censorship of Submarine Cables in Time of War," which noted this new exception to notice requirements and recommended that any suspensions or stoppages under Article 8 would be treated as "dangerous for the security of the State" and so no notice would ever be given.[82] In other words, it provided legal authority for secretive telegraph censorship and surveillance. The exception also effectively undermined the other indirect notice provisions established in 1875 – the refunds sent to senders for stoppages of their telegrams under Article 8 and 9. This is because for years the Service Regulations were changed – in a seemingly benign amendment by the then Commission of Regulations (which included Britain, among others) at an administrative telegraph conference in 1879 also, coincidentally, in London – providing that

---

[78] Documents of the International Telegraph Conference (1903), *supra* note 50, at 326, 669–72.

[79] *Id*. at 669–72.

[80] *Id*. at 670–72.

[81] *Id*. at 672.

[82] HEADRICK, *supra* note 20, at 98; Hills, *supra* note 44, at 199.

refunds would only be provided if they were demanded by the sender.[83] Without notice that their telegram has been stopped, it was difficult for the senders to make a demand.

The small 1903 exception, a seemingly minor compromise, undermined the system of checks established in 1875. By 1908, with the world creeping towards war, a secret British "Inter-Departmental Committee" was established to set up, and build, a system of "secret censorship."[84] Of course, Britain was not alone in making these moves towards covert telegram surveillance and censorship. The 1903 "exception" led to pervasive cable censorship, surveillance, and espionage during World War I, with state infrastructure created to conduct "war time" communications surveillance, cryptography, and censorship. After World War I, this became permanent or "peacetime" state surveillance or signal intelligence agencies.[85] For example, Britain's war time surveillance infrastructure would become a permanent peace-time agency in 1919 (called the Government Code and Cypher School); a department that would be expanded and renamed Government Communications Headquarters or GCHQ before the Second World War.[86]

Moreover, the Submarine Convention also neglected war times, and cable cutting between hostile states became increasingly common in the early 20th Century. In fact, submarine cable cutting was likely the first pre-meditated act of the First World War, when

---

[83] Documents of the International Telegraph Conference of London, 551 (1879), *available at* http://www.itu.int/dms_pub/itu-s/oth/02/01/S02010000054802PDFF.pdf.

The change in the language of Regulation LXVIII can be seen in the Official 1879 version of the Regulations (I have underlined the newly added text): "La taxe d'un télégramme arrêté en vertu des articles 7 et 8 de la Convention est remboursée à l'expéditeur, s'il en fait la demande, et le remboursement est à la charge de l'Administration qui a arrêté le télégramme." International Telegraph Convention (1875), Service Regulations, Tariffs, and Annexes, London Revision (1879), at Service Regulation LXVII, *available at* http://www.itu.int/dms_pub/itu-s/oth/02/01/S02010000054002PDFF.PDF (emphasis added).

[84] HEADRICK, *supra* note 20, at 98; Hills, *supra* note 44, at 199.

[85] Hills, *supra* note 44, at 197, 199–201 (noting particularly, that "secret" censorship and surveillance continued after the war).

[86] F.H. Hinsley & Alan Stripp, *Preface*, *in* CODEBREAKERS: THE INSIDE STORY OF BLETCHLEY PARK, at v (F.H. Hinsley & Alan Stripp eds., 1993) ("Just before the outbreak of the Second World War the Government Code and Cypher School (GC&CS) moved from London to Bletchley Park[,] . . . variously known as War Station X, . . . the Park, or Government Communications Headquarters (GCHQ) . . ."); *see* HEADRICK, *supra* note 20, at 219–24.

Britain and France cut German submarine cables spanning the Atlantic and North Sea on August 9, 1914.[87] Indeed, ambiguities and shortcomings in all of these international instruments rendered them inadequate to resist censorship, surveillance, or other cable communication disruptions. With no recourse under international treaty or convention, for example, non-state actors (i.e. companies) turned to litigation in national and international judicial forums to seek redress for cables damaged during war. For example, in the 1923 *Case of the Cuba Submarine Telegraph Company*, the British government (on behalf of British companies) famously brought a claim against the United States in the United Nations International Claims Tribunal, seeking compensation under customary international law principles for cables cut during the Spanish-American War. Though mostly unsuccessful, a few instances of high litigation did pressure or shame countries into settling damages.[88]

3.1.4. From Conflict and Control to Innovation

Though the Telegraph Convention was later revised, no agreement was ever settled upon to address telegraph communications at war. However, the idea that cable communications between neutral countries, even during wartime, were "inviolable" and thus should remain free of disruption was largely established. Articulated by the Institute of International Law in 1878, this principle had near universal acceptance[89] and was largely codified in Article 54 of the Fourth Hague Convention of 1907.[90] Britain, through its control over vast segments of the

[87] UNITED NATIONS, 6 REPORTS OF INTERNATIONAL ARBITRAL AWARDS 118 (2006), *available at* http://legal.un.org/riaa/cases/vol_VI/118-120_Cuba_Submarine.pdf (presenting the decision of Cuba Submarine Telegraph Co., Ltd. (Great Britain) v. United States (1923)).

[88] Higgins, *supra* note 21, at 30.

[89] R. J. R. Goffin, *Submarine Cables in Time of War*, 15 L.Q. REV. 145, 152 (1899) ("The only definite rule for practice that can be extracted from the conclusions of the Institute is that which declares cables connecting two neutral territories inviolable, a rule which would probably meet with universal acquiescence.").

[90] Convention (IV) Respecting the Laws and Customs of War on Land, Oct. 18, 1907, 187 C.T.S. 227, art. 54 ("Submarine cables connecting an occupied territory with a neutral territory shall not be seized or destroyed except in the case

international telegraph system, had established unchallenged supremacy in global communications during the First World War through its extensive telegraph infrastructure and secret programs of censorship – such that it could block or read "most secret messages of its enemies" but do so without detection or "revealing its sources."[91] This would represent the high-watermark of British strength in global communications, leading other states to look to new technologies – in particular the wireless telegraph – in attempt to "free themselves from dependence on foreign cables."[92] Indeed, innovation became the means by which the international community moved on from these information conflicts. Cable-based telegraph communications became less important in the years after the Great War, with the development of the wireless telegraph and radio communications.[93]

3.2. Case Study Two: High Frequency Radio Jamming

Freedom of information and radio jamming were major international issues after the Second World War. This prominence was due not only to U.S. influence – whose foreign policy was centered on First Amendment values – but also developments during the war itself.[94] Both war propaganda and state censorship, enabled by radio transmission jamming, were pervasive during the war and viewed by the world community as a serious threat to peace and stability.[95] The development of high frequency shortwave radio technology before the war – which made the transnational propagation of radio broadcasts possible – led countries like Germany to deploy a war strategy of "broadcast defense" involving systematic jamming of foreign radio stations.[96]

---

of absolute necessity. They must likewise be restored and compensation fixed when peace is made.").

91 HEADRICK, *supra* note 20, at 169.

92 HEADRICK, *supra* note 20, at 8.

93 Magder, *supra* note 36, ch. 2.

94 *See* Jonathon W. Penney, *Internet Access Rights: A Brief History and Intellectual Origins*, 38 WM. MITCHELL L. REV. 10, 21–22 (2011) (discussing the origins and history of the Free Flow of Information Paradigm).

95 *Id*. at 21–23.

96 *See* James G. Savage & Mark W. Zacher, *Free Flow Versus Prior Consent: The Jurisdictional Battle over International Telecommunications*, 42 INT'L J. 342, 344–47 (1987) (discussing broadcasting and deliberate indifference).

So, when state measures to control new radio technologies would eventually emerge in the Post-War Period, those efforts would be focused less on surveillance and more on disrupting and interfering with long range telecommunications. As we will see, international responses then attempted to respond in kind.

3.2.1. The Post War Consensus: The Free Flow of Information Doctrine

But first: the Post-War consensus. With the proliferation of the high frequency radio – making mass telecommunications possible – a strong consensus formed to promote the technology, through an international policy framework promoted by the U.S. and its allies: the "free flow of information" doctrine.[97] That is, the promotion of unrestricted global flows of information and ideas across state borders. The free flow doctrine, it was argued, could address state propaganda and censorship at the same time, undermining both with a diverse array of information sources.[98] The consensus on the free flow doctrine was reflected in the near complete absence of any radio jamming after the war.[99] It was also reflected in the wide range of international conventions, declarations, and agreements established at the time that codified the doctrine's principles, like the right to "seek, receive, and impart information" enshrined in article 19 of the United Nations' 1948 Universal Declaration of Human Rights (UDHR)[100] and the UN's 1946 Declaration on Freedom of Information – which declared information freedom a "fundamental human right" – adopted unanimously in the General Assembly's first session.[101]

---

97 Penney, *supra* note 93, at 23; *see generally* Savage & Zacher, *supra* note 96, at 348.

98 Penney, *supra* note 94, at 22–23.

99 Savage & Zacher, *supra* note 96, at 348 ("Immediately after the end of the war jamming was virtually absent from the air waves.").

100 Universal Declaration of Human Rights art. 19, G.A. Res. 217A (III), U.N. Doc. A/810 at 71 (1948) [hereinafter UDHR] ("Everyone has the right to . . . seek, receive and impart information and ideas through any media and regardless of frontiers.").

101 Calling of an International Conference on Freedom of Information, G.A. Res. 59 (I) (Dec. 14, 1946) [hereinafter Conference on Freedom of Information] ("Freedom of information is a fundamental human right and is the touchstone of all the freedoms to which the United Nations is consecrated"); Penney, *supra* note

3.2.2. From Consensus to Conflict and Control: Radio Jamming & Cold War Information Politics

This early Post War consensus on the free flow doctrine weakened as U.S.-Soviet relations began to deteriorate, after the Soviet Union began jamming U.S. radio broadcasts directed at Russia in 1948.[102] The Soviets, and their allies in the Eastern bloc, would continue to jam Western broadcasts, such as the BBC, Voice of America, Radio Free Europe, and Liberty Radio, for most of the Cold War.[103] Freedom of information would become a flashpoint for international legal disputes between East and West, with the West promoting the free flow of information and the Soviets advocating the sovereign right of states to restrict it.[104]

These struggles over information law and politics would take place across a vast range of international forums, including the International Telecommunications Union (ITU), UNESCO, and the UN General Assembly. Notwithstanding the West's success in

---

94, at 23–30; *see* CEES J. HAMELINK, THE POLITICS OF WORLD COMMUNICATION: A HUMAN RIGHTS PERSPECTIVE 60 (1994) (examining the global communication environment and the political process and decision-making that shape this environment).

[102] Savage & Zacher, *supra* note 96, at 348.

[103] Savage & Zacher, *supra* note 96, at 348 ("Immediately after the end of the war jamming was virtually absent from the air waves. However, in 1946 the Soviet Union began to jam Russian-language shortwave programmes from Franco's Spain. Following a significant deterioration in American-Soviet relations and the establishment of the Russian and East European language services of the Voice of America, the Soviet Union decided in late 1947 to commit a dozen transmitters to full-time jamming of the new VOA services. It began in February 1948."); Price, *supra* note 14, at 391; ("The Soviet Union began to jam Western radio broadcasts to the Soviet Union in 1948. . . . The prime targets of Soviet and East European jamming are the three major Western foreign broadcast stations, the BBC's External Broadcasting Services, the Voice of America (VOA), and Radio Free Europe/Radio Liberty (RFE/RL). . .") (footnotes omitted); Jamie F. Metzl, *Rwandan Genocide and the International Law of Radio Jamming*, 91 AM. J. INT'L. L. 628, 629 (1997) ("With the real and metaphorical fall of the Berlin Wall, this formerly neat division between sides became murkier. In 1988 Moscow ceased operation of its twenty-five hundred jamming stations and allowed Radio Free Europe and Voice of America broadcasts to flow in unimpeded. U.S. funding for such activities decreased dramatically. Control of the airwaves became a much less ideologically contested issue in international fora.") (foonotes omitted).

[104] *Id.* at 347–48.

having radio jamming prohibited and the free flow doctrine recognized in numerous international documents and forums – for example, every ITU resolution from 1947 onward condemned radio jamming – such measures did little to deter Soviet jamming activities, whom often cited national security justifications.[105] As with telegraph cable cutting, international law's failure to settle disputes over radio jamming and international broadcasting led some states and non-state actors to seek redress in alternative measures or forums, such as the International Frequency Registration Board (IFRB), the ITU's enforcement arm, which established both a global radio jamming monitor and a formal complaints process for states seeking redress.[106]

3.2.3. Additional International Measures: IFRB Radio Jamming Monitoring

The IFRB was initially set up to resolves disputes concerning interference with international broadcasts, and to administer and enforce the terms of the International Telecommunications Convention (ITC) and its annexed Radio Regulations.[107] But as is typically the case when international consensus breaks down over telecommunications policy, consensus-based institutions, such as the ITU, are paralyzed. Indeed, due to the divisive nature of Cold War international politics, the IFRB's strict enforcement capacity was seriously weakened.[108] However, one of the IFRB's more successful Cold War projects – which could have been a great long term international effort if given the chance – was its global "radio interference" or radio jamming monitoring program.[109] The

---

105 *Id*. at 343–44, 348, 362–63.

106 Savage & Zacher, *supra* note 96, at 355 (discussing that the U.S. used the IFRB in order to seek a settlement with the Soviet Union).

107 Price, *supra* note 14, at 402 n.28 ("The administration, enforcement and interpretation of this body of law is handled by the International Frequency Registration Board (IFRB).").

108 *See* Madelaine Eppenstein & Elizabeth J. Aisenberg, *Radio Propaganda in the Contexts of International Regulation and the Free Flow of Information as a Human Right*, 5 BROOK. J. INT'L L. 154, 158–59 (1979) (discussing the reality of international broadcasting regulations).

109 Savage & Zacher, *supra* note 96, at 362; *see* Bob Parnass, *Feds Finger Radio Jammers Again*, BELL LABS REPORT (1989), *available at* http://cd.textfiles.com/hamradio/swl/swlguid2/jammer.txt (discussing

program offers an intriguing role for international institutions to play – in particular the ITU – in relation to global telecommunications censorship and disruption, during periods of sustained international conflict about a technology or its governance.

Given the highly charged international disputes over radio jamming, few countries, other than the Soviet Union, went on the record as saying that they were deploying jamming. Thus, there was little information available about the location, scope, and spillover effects of jamming activities.[110] The IFRB's monitoring program was the first globally coordinated attempt to monitor and map those details, and was quite sophisticated, with the IFRB working with the National Telecommunications and Information Administration (NTIA) to use "radio direction finding equipment" and "HF monitoring" around the world to locate jammers.[111] The IFRB's radio jamming monitoring was established in response to Western lobbying at the ITU's 1984 High Frequency World

characteristics of the radio jamming monitoring program); *see* Bob Parnass, *Shortwave Jammers Identified*, BELL LABS REPORT (1987), *available at* ftp://69.43.38.172/mirrors/cd.textfiles.com/hamradio3/news/inham08/974 (raising questions as to whether using shielded cables on the computer reduces risk of static discharges from the body).

[110] Savage & Zacher, *supra* note 96, at 362; Parnass (1989), *supra* note 109; Parnass (1987), *supra* note 109.

[111] It took radio jamming to reach "record levels" in 1984 to spur the IFRB radio jamming monitoring program to be established. *See* MARY W. SOWERS & GREGORY R. HAND, NAT'L TELECOMM. & INFO. ADMIN., REPORT 90-262: MONITORING OF HARMFUL INTERFERENCE TO THE HF BROADCASTING SERVICE: SUMMARY OF MONITORING PROGRAMS HELD BETWEEN 1984 AND 1989 2–3 (1990) ("In 1984, broadcast services into the Soviet Union and Eastern Bloc countries were being jammed at record levels. The First Session of the World Administrative Radio Conference (WARC) for planning the frequencies allocated to the HF broadcasting service was held in February, 1984. This conference, designated WARC-HFBC(84), decided that coordinated worldwide monitoring programs to identify and locate sources of harmful interference to the HF broadcast service be initiated under the auspices of the International Frequency Registration Board (IFRB) . . . . The National Telecommunications and Information Administration's (NTIA) Institute for Telecommunication Sciences (ITS) led a highly coordinated effort using HF monitoring and radio direction finding equipment located around the world to determine the 1ocation and extent of jamming to international broadcast services."). The author is aware of no other global radio jamming monitoring program undertaken by the ITU or any comparable international body. For a discussion of the "planning principles and technical parameters" of the monitoring program, see Charles Rush, George Jacobs & Warren Richards, *The Results of WARC-HFBC(87): Technical Implications*, 34 IEEE TRANSACTIONS ON BROADCASTING 102 (1988).

Administrative Radio Conference (HF-WARC).[112] Radio broadcasts were being jammed around the world in 1984 at "record levels," with no real recourse for states or international broadcasters under treaty or convention.[113] Perhaps seeking alternative means to fight the jamming activities, Western governments persuaded the HF-WARC to issue a resolution requesting the IFRB to monitor and report on radio jamming around the world.[114]

The IFRB, working jointly with the U.S. National Telecommunications and Information Administration (NTIA), established a globally coordinated effort to monitor the location and extent of international radio broadcast jamming worldwide.[115] In reports issued in 1985, 1986, and 1987, the IRFB set out the location of 100 sources of global radio jamming, and found most of these sites were located in Soviet or Eastern bloc country territory.[116] These reports were tabled at the 1987 HF-WARC, formally confirming radio-jamming activities being conducted by the Soviet Union, Bulgaria, Czechoslovakia, and Poland, as well as a number of smaller developing countries. The aim was to stir more international pressure on jamming countries to cease, or at least scale back, their activities.[117] Interestingly, by the time of the second session of the 1987 HF broadcast conferences, jamming had "diminished considerably."[118] Though certain Western broadcasts such as Voice of America remained jammed for various languages in the USSR, jamming activities in smaller Eastern bloc were significantly scaled back, and in some countries like Poland, they ceased completely.[119]

As with other instances in which jamming activities received international attention, the Soviet government was undeterred. Smaller states, such as developing countries or those in the Eastern

---

112 Savage & Zacher, *supra* note 96, at 361–62 ("The matter was tackled again at the opening session of the High Frequency-World Administrative Radio Conference (HF- WARC) of 1984 and as a result of Western prodding, a resolution was passed requesting the IFRB to monitor and report on jamming activities.").

113 SOWERS & HAND, *supra* note 111, at 2.

114 Savage & Zacher, *supra* note 96, at 361–62.

115 *Id*. at 2–3.

116 *Id*. at 2–3.

117 Savage & Zacher, *supra* note 96, at 362.

118 SOWERS & HAND, *supra* note 111, at 2–3.

119 SOWERS & HAND, *supra* note 111, at 2–3.

bloc, became increasingly responsive to monitoring. They may, as James Savage and Mark Zacher have suggested, have felt "constrained from jamming because of cost or the possible damage to their reputations . . . ."[120] With a global platform, the ITU program imposed a significant reputational cost for radio jamming, creating a greater deterrent effect. Of course, there were other complex factors at play here with Cold War tensions easing by the late 1980s.[121] Yet IFRB monitoring and reporting, with its robust methodology and technical sophistication,[122] constituted the "gold standard" in radio jamming tracking, with its high profile reports likely seen as both sufficiently credible and objective to impact reputation – a Cold War precursor to contemporary efforts to map and track global Internet censorship.

Beyond such censorship monitoring, international law, however, again offered little recourse for victims of censorship and jamming, leading states and interested parties on either side of the Cold War radio jamming divide, to pursue other avenues. One avenue or measure for recourse was the IFRB complaints process. Although, as earlier noted, the IFRB had little actual enforcement capability, its pronouncements nevertheless brought to bear some pressure on states acting in breach of the ITU Convention and Radio Regulations. This was apparent in the radio jamming disputes between Cuba and the United States. In the 1960s, Cuba began jamming radio broadcasts originating in the southern U.S., and would do so, off and on, for most of the Cold War.[123] Though there was some concern that the disputes would lead to a military confrontation, no conflict materialized. Instead, both countries, among other actions, utilized international and national formal complaints processes.[124] Both, for example, lodged formal complaints against each other with the IFRB, which would investigate and issue compliance rulings in response to complaints that state governments, or non-state actors in state territories, were violating ITC rules or regulations. Cuba also lodged complaints

---

120 Savage & Zacher, *supra* note 96, at 362.

121 *See* Parnass (1989), *supra* note 109 (noting that "closer" East/West relations led to a decrease in jamming).

122 *See generally* SOWERS & HAND, *supra* note 111 (describing the methodology of the IRFB reports); Parnass (1987), *supra* note 109.

123 Savage & Zacher, *supra* note 96, at 350.

124 Omar Javier Arcia, *War over the Airwaves: A Comparative Analysis of U.S. and Cuban Views on International Law and Policy Governing Transnational Broadcasts*, 5 J. TRANSNAT'L L. & POL'Y 199, 203–05 (1996).

with the U.S. Government about anti-Fidel Castro radio broadcasts being transmitted into Cuba, with some leading to FCC action to shut down un-licensed pirate radio broadcasts.[125]

Both countries achieved some success with these complaints. Though the IFRB was unable to enforce its findings, its investigations into Cuban radio jamming pushed the Cuban government to the negotiating table in various international forums,[126] and overall, Cuban jamming efforts were never more "than limited and half-hearted."[127] From the Cuban standpoint, the FCC closed down anti-communist and anti-Castro pirate radio states in Florida in 1980 in response to their complaints.[128] Much like the less powerful developing and Eastern bloc countries that the IFRB's monitoring program exposed, Cuba appeared responsive to bad press and international exposure for its jamming activities.

---

[125] *Id.* at 202. Hazel G. Warlaumont, *Strategies in International Radio Wars: A Comparative Approach*, 32 J. BROAD. & ELEC. MEDIA 43, 51 (1988) ("The U.S. and Cuba held bilateral talks on radio interference before and after the 1981 Rio Conference, and even during the tense times when Radio Marti was introduced both the U.S. and Cuba engaged in some diplomatic activities. For instance, Cuba sent the U.S. a formal written protest about Radio Marti and the U.S. sent a private envoy to Havana attempting to soften the impact of the new program . . ."); William Labbee, *Cuba Over and Out*, MIAMI NEW TIMES (Nov. 21, 1990), http://www.miaminewtimes.com/news/cuba-over-and-out-6365139 ("Coincidentally, listeners in Miami neighborhoods and Cuban cities, towns, and villages tuned in their short-wave sets four days per week to hear the gravelly voice of Comandante David, who claimed to be broadcasting from somewhere on the island and who called for the overthrow of Fidel Castro in explosive diatribes against the dictator. . . . So began the most-celebrated case involving anti-Castro clandestine radio in the U.S., a case that eventually would lead to ten years of pursuits and disputes between the FCC and broadcasters, between Cuba and the U.S. government, and between the FCC and the White House. Castro complained to the U.S. government about David in late 1979, and by early 1980 the FCC had pinpointed the radio signal to a house at 8780 SW 51st St., the residence of Jose M. Gonzalez, a 47-year-old exile from Santa Clara, Cuba. Agents warned Gonzalez to quit broadcasting, but the ten- to fifteen-minute programs, broadcast on Monday, Wednesday, and Friday nights and on Sunday afternoons, continued unabated, including references to attempts to shut down the transmissions. U.S. marshals twice raided Gonzalez's house in 1980, confiscating broadcasting equipment.").

[126] *Id.* at 204.

[127] Savage & Zacher, *supra* note 96, at 350.

[128] *See generally* Arcia, *supra* note 124, at 202; Warlaumont, *supra* note 125, at 53; Labbee, *supra* note 125.

3.3. Case Study Three: Direct Broadcast Satellite TV Jamming

Once again, new innovations pushed the "cycle" into a different stage: namely, the development of communications satellites drove international telecommunications and debates into new regulatory controversies. Thus, our final case study of global telecommunications disruption concerns international disputes over direct-to-receiver satellite broadcasting, or direct broadcast satellite (DBS), in the 1970s.

3.3.1. The COMSAT Consensus

When communications satellites first went online in the 1950s and 1960s, the world community's initial response was, unsurprisingly, very positive. There was a strong consensus about the great potential for global satellite communications, including the opening up of a new frontier for exploration: space.[129] This idealism, like past consensus about the telegraph or radio, would be reflected in international norms, particularly the 1967 Treaty on Outer Space, which reflected these ideals and was supported by the most important world powers at the time: the U.S., Russia, and the United Kingdom. The Treaty declared "space" a neutral zone and a common space for all humanity.[130]

---

[129] *See* Eilene Galloway, *Direct Broadcast Satellites and Space Law,* 3 J. SPACE L. 3, 3 (1975) (emphasizing the great benefits to "mankind" of satellite being effectively recognized in the 1967 Treaty on Outer Space); *see also* Nancy M. Lesko, *Legal Implications of Direct Satellite Broadcasting – The UN Working Group*, 6 GA. J. INT'L & COMP. L. 564, 564 (1976) (speaking of satellite fostered changes as the "greatest technological revolution in history. . .").

[130] Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, G.A. Res. 2222 (XXI), *opened for signature* Jan. 27, 1967, 18 U.S.T. 2410, 610 U.N.T.S. 205 (entered into force Oct. 10, 1967) ("Outer space . . . shall be free for exploration and use by all States . . . on a basis of equality and in accordance with international law, and there shall be free access to all areas of celestial bodies."). *See also* Galloway, *supra* note 129, at 3 (noting that space increased man's knowledge of the universal and had practical implications for all of humanity); Lesko, *supra* note 129, at 564 (stressing that the world community must acknowledge the interdependence of the legal and technical aspects of DBS).

3.3.2. From Consensus to Conflict and Control

Like other global telecommunications technologies, the international consensus about satellite communications did not last. In fact, the seeds of its demise were already planted by the late 1960s, as DBS was being developed.[131] DBS provided the capability to beam television signals directly to targeted populations across national borders.[132] Eventually, states around the world began to understand the true potential – and threat – posed by satellite telecommunications technology, in this form.[133] Not surprisingly, DBS stirred international controversy and, like other global communications conflicts during the Cold War, led to disputes about the legality of states blocking or jamming DBS signals.[134] The COMSAT consensus had broken down, leading to conflict and attempts at control. Early on, international lawyers and legal scholars questioned whether traditional "state sovereignty" justifications for communications jamming – based on theories of territorial control over airwaves or national security – could justify satellite jamming or blocking.[135] Since satellites operated far beyond the airspace that international law recognized as subject to territorial control, the airwave theory was inapplicable.[136] The national security justification was also weak, given that satellite jamming often meant interfering with the

131 *See* Lesko, *supra* note 129, at 564–65 (observing that the Treaty on Outer Space failed to deal with the more "difficult" earthbound activities, including direct broadcast satellite).

132 Galloway, *supra* note 129, at 15–16 (noting transmission directly to private sets); Lesko, *supra* note 129, at 565 (pointing out the rapid rise of such technology).

133 Galloway, *supra* note 129, at 15–16 (describing several international controversies around DBS); Savage & Zacher, *supra* note 96, at 344; Lesko, *supra* note 129, at 565–66.

134 Savage & Zacher, *supra* note 96, at 357.

135 Samuel D. Estep & Amalya L Kearse, *Space Communications and the Law: Adequate International Control After 1963?*, 60 MICH. L. REV. 873, 877–79 (1962) ("The general consensus of the majority of jurists is that existing international agreements recognize the sovereignty of a state over its superjacent 'airspace,' and that space beyond the earth's atmosphere is not included. . . . The first such problem presented is the choice between the theories upon which a state may claim the right to jam a 'transgressing' radio signal. Neither the sovereignty-over-airspace theory nor the national security theory is entirely satisfactory, both allowing jamming in instances which seem not to justify interference. . .") (footnotes omitted).

136 *Id*. at 877.

capabilities of the satellite itself, preventing it from broadcasting at all.[137]

These questions concerning the legality of regulating or jamming DBS, led to good faith international efforts to negotiate a treaty to cover DBS communications and transmissions.[138] However, international law largely gave way to international politics. In contrast to the East-West divide on radio jamming, the politics of DBS were complex. Television's cultural and political power far exceeded radio, and many states perceived DBS as a threat to national control over television broadcasting.[139] Nations subsequently divided along three lines over DBS: the U.S. and some developed Western countries advocated for the free flow of communications, the Soviet and its Eastern bloc allies pushed for full jamming powers, and a third group of countries, mainly developing nations, supported more moderate regulatory powers over DBS transmissions.[140] This new regulatory coalition – between the "East" and "South" – was successful in promoting its agenda in various international forums, such as the ITU, UNESCO, and the UN General Assembly. For example, it achieved some recognition for the concept of "prior consent," that is, DBS should not be transmitted into a state's territory without its prior consent in a General Assembly resolution in 1972, with 102 voting in support and only the United States voting against.[141] This was later referred to as the "Jammers Charter."[142] Though never formalized, the notion of prior consent only complicated relevant law and weakened the case for free flow of information principles.

4. UNDERSTANDING THE "CYCLES" (IF THEY EVEN EXIST. . .)

Beyond a historical examination of global communications disruption, surveillance, or censorship, do these cases offer any insights, lessons, or implications for Internet censorship resistance

---

137 *Id*. at 878.

138 *Id.* at 877–79. *See also* Juliana Maio, *Direct Broadcasting by Satellite: A Domestic and International Legal Controversy*, 1 COMMENT L.S. 193 (1978).

139 Lesko, *supra* note 129, at 567–68 (noting controversy over "cultural propaganda"); Savage & Zacher, *supra* note 96, at 344–45.

140 Savage & Zacher, *supra* note 96, at 357–59.

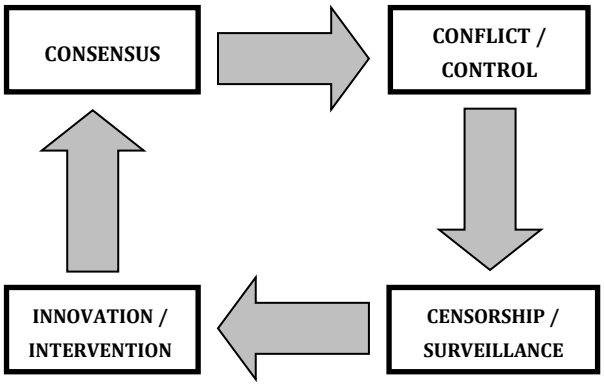
141 *Id*. at 359.

142 *Id*. at 359.

today? I believe so. A central question Wu poses in *Master Switch* is "Will this time be different?" That is, will the Internet, perhaps the most powerful global telecommunications technology yet, regress toward the seeming "inevitable" pattern of information industries before it: a move to monopoly, centralization, and ultimate closure?[143] Wu is not certain as to the right answer – and gives some reason for both optimism *and* pessimism – while suggesting vigilance to "preserve [the Internet's] openness from imperial designs."[144]

These case studies do not provide an answer either, but they do add an important layer of international complexity to Wu's question, suggesting comparable regulatory patterns but with distinctive features, given their global or international context. This, itself, offers some important insight into the regulatory challenges that global telecommunications technologies, like the Internet, are most likely to face. If we were to adopt Wu's framework to a global communications level, it would likely look something like **Figure 1.2**.

Figure 1.2
Do the Case Studies Support this Adaption of Wu's "Cycle" in the Global Telecommunications Context?



Yet, answering Wu's question arguably also requires more than

143 WU, *supra* note 3, at 6, 316–19.

144 WU, *supra* note 3, at 318.

merely adopting or mapping his theory onto global technologies. To explore that problem at the very least requires understanding the nature of the regulatory challenge.

The analysis thus far of the three case studies certainly provides some support for Wu's notion of regulatory cycles on a global stage, as seen in **Figure 1.2**. At the same time, however, one could also take issue with the uniformity of how the "patterns" are represented. There was certainly a "consensus" period concerning both the telegraph in the mid-19th Century and the shortwave radio after the Second World War, but both were remarkably brief; the same could be said for the "COMSAT" consensus concerning communication satellites.[145] The rest of the time, states competed both offensively and defensively in relation to the given global telecommunications technology. One could say these brief prosperous periods were marked less by the goodwill of powers, and more by the ignorance of states about the strategic value of the technology in question. Yet, once that value was realized, they quickly worked to undermine international legal measures meant to protect and promote the technology to their own strategic advantage. This can certainly be said of the international telegraph system – Britain did not fully appreciate its value until the very late 19th Century, arguably not until after the Spanish-American and Boer Wars.[146] Likewise, Americans in the Post-War period believed that broadcasting Voice of America and Radio Free Europe to Soviet states had strategic value, while the Soviets obviously believed radio-jamming benefitted them.[147]

Certainly, some neo-realist theorists of international relations would posit that any goodwill or consensus was merely a myth, and that a better representation would simply be (1) the

---

145 *See supra* notes 97–104, 129–35 and accompanying text.

146 *See supra* notes 63–64 and accompanying text.

147 *See supra* notes 102–03 and accompanying text; Warlaumont, *supra* note 125, at 46–47 ("The radio war between the U.S. and the Soviet Union was intense during times of crisis and appeared to ebb during times of détente. It was characterized by a pattern of U.S. broadcasting and Soviet jamming. In addition, both nations broadcast in many languages around the world competing for supporters in the cold-war ideological debate . . . . Preventing or jamming incoming broadcasts is important to nations attempting to maintain strict control and who use the media primarily to support party goals. Both Cuba and the U.S.S.R. operate under systems that advocate the control of information. In the radio war between the U.S. and the Soviet Union, jamming has often proved to be an effective strategy because Soviet listeners do not have easy access to information from other sources . . .") (citations omitted).

introduction of a new technology and (2) a competition among states internationally to use the technology to their strategic or commercial advantage.[148] While there is some evidence of this among the three case studies, I also do not think this is an accurate understanding of the regulatory "patterns" or cycles examined. The reality is that there was a period of consensus about the telegraph that led to an impressive and wholly progressive – for the period – international legal regime, as represented by the 1875 International Telegraph Convention. Similarly, there was a period in the Post War Period where radio jamming was almost non-existent and, with the introduction of satellite communications technology, a positive vision shared by the international community led to the strikingly positive 1967 Treaty on Outer Space.[149] A strictly neo-realist view of these case studies cannot account for these realities. Then again, certainly it was use and abuse of communications technologies that often led to greater telecommunications control and disruption or, on the other hand, a push to innovation so as to avoid such challenges.

Moreover, another central theme relating to the brief moments of consensus and goodwill is that the international legal rules, regulations, policies, or institutions adopted during the brief periods of consensus, and employed with a more cooperative aim, led, not surprisingly, to more robust and effective international legal measures for protecting global communications from censorship, surveillance, disruption, and control. The Submarine Cable Convention and the International Telegraph Convention (at least its 1875 version) were strong, even visionary, international legal schemes with noticeable weaknesses – a failure to address times of war.[150] Similarly, the many international legal instruments and documents forged in the Post War Period that reflected and promoted the "free flow of information" are among the most

---

148 *See* Nye, *supra* note 1 (offering some rebuttal to strictly neo-realist contentions in the Internet space in the context of "cyberpower").

149 *See supra* notes 97–104, 129–30 and accompanying text.

150 Convention for the Protection of Submarine Telegraph Cables, Mar. 14, 1884, 163 C.T.S. 241 (entered into force May 1, 1888); *see also supra* notes 87–88 and accompanying text. The Convention for the Protection of Submarine Telegraph Cables, like the 1875 Telegraph Convention, was innovative in that it took individuals as its focus or subject matter, a rarity in international law in the period. On this point, see *supra* note 42 and accompanying text. *See also* Kelsen, *supra* note 62, at 537–38 (noting that the Convention directly obligated individuals).

important international legal tools from which are found not only communication rights, but also universal human rights more generally. Finally, the Treaty on Outer Space of 1967 declared and protected space from war and hostilities for the ensuing decades;[151] space remains just as peaceful today.

So, while healthy skepticism about a perfectly congruous "Cycle" is warranted, the historical parallels are at least worth considering, both from an historical perspective but also from the perspective of present legal and policy challenges concerning the Internet.

4.1. Has the Internet Had Its "Boer War" Moment?

This leads us back to Wu's question about the Internet. One possibility, in light of these case studies, is that the Internet may have already experienced its "Boer War" moment. What does this mean? The Boer War, ending in 1900, was an important and consequential turning point in the fate and future direction of the international telegraph system, at least in terms of its regulation and control by states. Britain's overreaching and questionable use of Article 8 powers for broad cable censorship, surveillance, and control sent shockwaves among the other world powers about the clear strategic asset the telegraph had become in Britain's hands. [152] Up until that point, the world community seemed to view the telegraph as a tool for global prosperity and commercial growth, with most states happy to let Britain take the lead in its expansion and governance through private enterprise.[153]

However, from the Boer War onward, it was understood as a strategic asset and a potentially powerful instrument of war. States would compete and move to strengthen their own position in the international telegraph system through investment in infrastructure both to break Britain's hold and to re-shape the international regulatory regime governing the International Telegraph System to their advantage. States would work to "free themselves from dependence on foreign cables" and state cryptanalysis capabilities, not only to protect the secrecy of their

151 *See supra* note 130 and accompanying text.

152 *See supra* notes 64–66 and accompanying text.

153 *See supra* notes 70–71 and accompanying text.

own messages, but also to break the codes of other competing states.[154] The international telegraph system would never be the same after the revelations of the Boer War; any goodwill or consensus disintegrated into competition and control.

Concerning the Internet, we have likely already left any period of consensus concerning Internet regulation and governance. Certainly, states have censored and monitored the Internet for years,[155] which is clear evidence that many countries have long understood the Internet's potential as either an offensive technology or as a threat to national security, stability, or some other national interest. Arguably, however, we have entered an even more acute stage of information conflict and control. First, as noted at the outset, states have been ramping up "cyberwar" capabilities in recent years, such as the U.S. National Cybersecurity Center established in June 2009.[156] Other countries have followed suit, creating the semblance of an international race to develop information security capabilities, both offensively and defensively. Second, until now, there had not been so many sustained and coordinated international efforts to deploy international institutions, law, or regulations to control or regulate the telecommunications technology.[157] That may be the backstory to the ITU's 2012 controversial World Conference on International Telecommunications (WCIT-12) this past December.[158] The

---

154 HEADRICK, *supra* note 20, at 219–24.

155 The ONI has been tracking Internet censorship since 2003. Oni Team, *Global Internet Filtering in 2012 at a Glance*, OPENNET INITIATIVE BLOG (Apr. 3, 2012), http://opennet.net/blog/2012/04/global-internet-filtering-2012-glance.

156 Hull et al., *supra* note 1, at 41–32; *see generally* Geers, *supra* note 1.

157 This is likely due to the increasing use of cyber-weapons and cyber-warfare by Governments, and the growing role for international bodies like the UN and ITU in Internet governance. States like China, Russia, and other Internet censors see such international forums as helpful mechanisms to "legitimize" their vision for a controlled Internet. RON J. DEIBERT, BLACK CODE: INSIDE THE BATTLE FOR CYBERSPACE 173–74 (2013).

158 *See* Richi Jennings, *Victory! UN/ITU Powergrab Thwarted at WCIT*, COMPUTERWORLD (Dec. 14, 2012, 6:20 AM), http://blogs.computerworld.com/internet/21500/victory-unitu-internet-power-grab-thwarted-wcit-itbwcw (describing the WCIT treaty as controversial and noting that a number of countries refused to sign it); Jeremy Fleming, *UN Chief Warns 'New Cold War' Looms over the Internet*, EURACTIVE.COM (Feb. 28 2013, 8:13 AM), http://www.euractiv.com/specialreport-mobile-broadband/un-chief-warns-new-cold-war-blow-news-518118 ("[T]he EU joined the United States and Canada in refusing to sign up to the treaty changes, creating a divide with the rest of the world.").

meeting, its looming threat of an Internet "takeover," either through regulation or transferring ICANN's Internet governance responsibilities to the ITU, and its deeply divided conclusion (a vote split nearly down the middle) suggest any consensus about Internet governance and regulation is behind us.[159]

While each of these developments is important, if there was any moment for the Internet comparable to the revelations of the Boer War and the telegraph, it was the National Security Agency revelations of 2013. The NSA's large scale Internet and telecommunications surveillance – through programs like PRISM, decryption methods, and other means[160] – and international reactions thereto,[161] likely mean global efforts to censor, control, or monitor the Internet will only grow in both intensity and scope.

5. BREAKING THE REGULATORY PATTERNS?

5.1. Censorship & Surveillance Resistance: International Legal Foundations

Things may not be all dark. No pattern or cycle is inevitable and arguably, with each new technology, efforts to understand and resist regulation and control by states will have both historical precedent and existing infrastructure, including international legal rules, from which to learn. As already argued, for example, these leftover and remaining international legal rules and institutions adopted during the brief periods of consensus cooperation, may

---

159 *Id*.

160 See sources cited *supra* note 1, with respect to "increasing" surveillance capabilities. See *infra* note 161 for sources concerning PRISM.

161 *See* Didier Bigo, Gertjan Boulet, Caspar Bowden, Sergio Carrera, Elspeth Guild, Nicholas Hernanz, Paul de Hert, Julien Jeandesboz & Amandine Scherrer, *Open Season for Data Fishing on the Web: The Challenges of the US Prism Programme for the EU,* CEPS POLICY BRIEF NO. 293 (June 18, 2013) ("The revelation of the top-secret US intelligence-led PRISM programme has triggered wide-ranging debates across Europe"); Jedidiah Bracy, *The NSA's PRISM Program and Reactions*, THE PRIVACY ADVISOR, THE INT'L ASS'N OF PRIVACY PROF'L (June 7, 2013), https://www.privacyassociation.org/publications/the_nsas_prism_program_and_reactions (observing that the "revelations about Verizon and the NSA[] is affecting talks between the EU and U.S. on a data protection agreement") (citation omitted); Editorial, *Worldwide Reaction to NSA/PRISM Surveillance – An Overview*, INFOSECURITY MAG. (June 12, 2013), http://www.infosecurity-magazine.com/view/32901/worldwide-reaction-to-nsaprism-surveillance-an-overview/.

lead to more robust and effective protections for global telecommunications. Indeed, these case studies also have important legal and policy lessons for those aiming to implement new state mass surveillance practices, and for those aiming to resist such practices.

With the U.S. Government announcing cyber-deterrence measures, and countries like China and Iran ramping up both cyber-security and Internet censorship capabilities in response, geo-politics once again permeate and complicate global communications policy, much as they did for telegraph, radio, and satellite communications. Within this broader geo-political context, critics have questioned the legitimacy of "Internet freedom" and related activities like Internet censorship or surveillance resistance.[162] These criticisms often have both a legal and political component, questioning how state or non-state actors can justify censorship circumvention tools that supposedly undermine national laws that implement local security or cultural policy preferences (and are presumably enforced by Internet filtering or censorship regimes).

5.1.1. A Reasonable Legal Foundation

Notwithstanding uncertainty as to the legality of different forms of communications, censorship under international law, a reasonable and legitimate legal basis for Internet censorship or surveillance circumvention, and related activities, can be easily articulated. Internet censorship or surveillance resistance activities help promote important and recognized international legal rights and principles, like freedom of information, freedom of expression, and the right to "seek, receive and impart information . . . ."[163] All of these values have been recognized under international law in a broad range of treaties, conventions, international legal precedents, and declarations, many of which were discussed above, such as the UN Declaration on Freedom of Information,[164] Article 19 of the UN's 1966 International Covenant on Civil and Political Rights,[165]

---

162 *See supra* note 12 and accompanying text.

163 UDHR, *supra* note 100, art. 19.

164 Conference on Freedom of Information, *supra* note 101.

165 International Covenant on Civil and Political Rights, Dec. 16, 1666, 999 U.N.T.S. 171, 6 I.L.M. 368.

and the UN's 1948 Universal Declaration of Human Rights, the latter of which is today largely understood to represent customary international law, rendering it binding on all states.[166]

Moreover, the panoply of international telecommunication conventions, regulations, and resolutions has condemned communication disruption and censorship – across a variety of technologies like those herein discussed – throughout the twentieth century. Internet censorship resistance activities, engaged by both state and non-state actors, is also consistent with the principles of the free flow of information doctrine – a policy that had near unanimous international support in the post war years.[167] Although this consensus weakened over time, the free flow doctrine still retains influence and wide international support.[168] While international disputes over the legality of global communications disruption and censorship left many questions unanswered, those efforts led to the important recognition and codification of international legal principles that provide a reasonable legal foundation for Internet censorship resistance today.

5.2. National Security Justifications and Their Limits

Critics would no doubt counter, as earlier discussed, that Internet censorship or surveillance circumvention – both state and non-state efforts like BBC World Service's effort to deliver online content to heavily censored regions[169] – undermines national laws

---

166 UDHR, *supra* note 100, art. 19.

167 *See supra* notes 97–110 and accompanying text.

168 Penney, *supra* note 94, at 25, 29–31 (noting that the "Free Flow of Information Paradigm, largely advocated by the United States and other Western countries, remained influential at the international level for decades after the Post-War years"; later demonstrating how each element of the "free flow of information doctrine" can be found reflected in a recent report on internet access rights by Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression).

169 KARL KATHURIA ET AL., CANADA CTR. FOR GLOBAL SEC. STUD. & CITIZEN LAB, UNIV. OF TORONTO, CASTING A WIDER NET: LESSONS LEARNED IN DELIVERING BBC CONTENT ON THE CENSORED INTERNET (2011), *available at* http://www.munkschool.utoronto.ca/downloads/casting.pdf (noting that "The restrictive communications environment and legal and regulatory frameworks in China and Iran, coupled with the regimes' tendency to adapt information controls to sensitive events, makes them challenging markets for delivering news content

reflecting local culture, morality, and security, which are enforced by Internet filtering and censorship. Justifications based on public morality or security arise from the principle of state sovereignty – a bedrock of international law. While state sovereignty is a fundamental international legal principle, our case studies also offer insight as to how far the principle can be stretched to justify censorship or surveillance. To begin with, policing local morality is often cited as a basis for Internet censorship or filtering – and modern international legal documents often include as a potential limit on free expression – but it was historically limited in scope.[170] In the 1875 Telegraph Convention, no private telegram could be blocked or prevented from reaching its destination for reasons of morality, decency, or even public order without also notifying the sender.[171] In practice, after the 1903 revisions, states like Britain dubiously utilized Article 8 stoppage and its notice exception to circumvent Article 7 – yet the mandatory notice requirements remain.[172] With the rise of satellite and radio communications, the most common "state sovereignty" theories supposedly justifying jamming activities were not based on public morality, but control over airspace or national security, with the latter being the most robust. National security has long been the most compelling justification for telecommunication censorship and surveillance regimes.[173]

However, the national security justification has also experienced historical limits. For example, before the Telegraph Convention's Service Regulations were revised in 1903, no private or state telegram could be blocked for national security reasons without also immediately notifying its sender,[174] which frustrated

---

and suitable test beds for assessing strategies for bypassing censorship to ensure news delivery."). *Id.* at 24.

170 *See supra* notes 97–110 and accompanying text.

171 *See supra* notes 43–54 and accompanying text.

172 Admittedly, states move to regulate the use of secret codes during war, as even with decryption capabilities, surveillance was difficult and time consuming. *See* CHARLES M. DOLLAR & JOAN R. GUNDERSON, AMERICA, CHANGING TIMES 853 (2d ed. 1982) (stating that "*[m]uch of this work of deciphering messages (1914-1918) was laborious and time consuming, still based largely upon frequency analysis. . .*"); DAVID PAULL NICKLES, UNDER THE WIRE: HOW THE TELEGRAPH CHANGED DIPLOMACY 181 (1st ed. 2003) (discussing how U.S. State Department officials found it difficult to decode their own coded cables).

173 *See generally* Hills, *supra* note 44, at 195 (arguing that the basis for censorship has almost always been perceived threats to national security).

174 *See supra* notes 43–54 and accompanying text.

the purpose of secret cable surveillance and censorship. Even under the 1903 London revisions, national security censorship was limited – only State telegrams (not private) could be legally "suspended" without notification, and only if such notice would pose a "dangerous" threat to national security (e.g., when the sending State and blocking State were at war).[175] During international debates about DBS communications, scholars questioned whether theories of national security based on customary international legal principles could justify satellite jamming.[176] This conversation led to international efforts to negotiate a new treaty to cover satellite communications and its regulation. In other words, these case studies suggest that the most cited justifications for Internet censorship may not have been as broad as commonly described or understood today.

5.3. Alien Torts, Internet Intermediaries, and Expanding International Legal Liabilities and Risks

An additional historical insight from these case studies is the potential for national or international litigation over transnational telecommunications disputes. In the past, state and non-state actors sought redress over communication related disputes or injuries through other means such as litigation when there was insufficient or uncertain international enforcement or protection.[177] Occasionally, as with British companies seeking redress for telegraph cable cutting, this involved national or international litigation.[178] But with radio jamming, states began to file formal complaints or claims with national or international bodies or

---

[175] The 1903 regulation changes allowed for Article 8 "suspension" of the telegram service (for the service as a whole, or for certain classes of correspondence) without notice to the sender if providing notice posed a danger to national security. However, notice requirements for Article 7 stoppages of private telegrams remained in place. *See supra* notes 43–54, 77–86 and accompanying text.

[176] *See supra* notes 135–37 and accompanying text.

[177] For example, see the discussion of the 1923 *Case of the Cuba Submarine Telegraph Company*, wherein British companies sought redress through litigation against the United States for cutting British submarine cables during the Spanish American war. *See supra* notes 87–88, 123–28 and accompanying text.

[178] *See supra* notes 87–88 and accompanying text.

tribunals.[179]

Avoiding potential entanglement in international disputes and related litigation between states may be one good reason for organizations involved with Internet censorship resistance to shun official state sponsorship. As with the radio jamming, officially sponsored U.S. radio broadcasts were specifically targeted by foreign jammers, and were the subject of complaints lodged in international forums.[180] Of course, shunning state sponsorship may also leave an organization vulnerable to legal complaints from foreign governments. For example, the FCC shut down non-licensed pirate radio stations in Miami in response to complaints from the Cuban Government.[181]

The current potential for litigation over state censorship and surveillance online – and related issues like surveillance technology, censorship circumvention, and human rights – is even more acute with recent trends in both international law and U.S. federal law. Indeed, international law has evolved in recent decades through new legal rights, added responsibilities, and potential liabilities for non-state actors like corporations and organizations.[182] These changes, combined with other evolutions in domestic U.S. law – such as the growth of legal claims for violations of international law brought under the Alien Tort Statute (ATS) – has created a new minefield of potential liabilities for U.S. Internet intermediaries and technology companies, as well as organizations engaged in transnational Internet related activities abroad.[183]

ATS – a simple statute passed in 1789[184] – was likely meant to afford foreign plaintiffs, such as merchants and ambassadors, the right to sue American citizens in U.S. courts for violations of international law and for causing injury to person or property.[185]

---

179 *See supra* notes 123–28 and accompanying text.

180 *See supra* notes 103–04, 123–28, 147 and accompanying text.

181 *See supra* notes 125 and accompanying text.

182 Censorship and surveillance resistance are closely related because Internet surveillance and monitoring likely causes users to censor their speech or other activities online. *See* Roger P. Alford, *Apportioning Responsibility Among Joint Tortfeasors for International Law Violations*, 38 PEPP. L. REV. 223, 223–24 (2011) (discussing changes in modern international law).

183 *Id*. at 235; Alien Tort Statute, 28 U.S.C. § 1350 (2006) [hereinafter ATS].

184 ATS, *supra* note 183. The ATS was part of the Judiciary Act of 1789, 1 Stat. 73, § 9 (1789).

185 Gary C. Hufbauer & Nicholas K. Mitrokostas, *International Implications of the Alien Torts Statute*, 7 J. INT'L ECON. L. 245, 246 (2004).

Today, ATS allows for a broader range of international claims. With increasing numbers of successful plaintiffs obtaining judgments and settlements, ATS awards range from $1.5 million to $766 million in compensatory damages, and have been as high as $1.2 billion in punitive damages.[186] A central concern here is that U.S. companies and organizations may eventually be found liable under ATS for aiding and abetting human rights abuses, or other breaches of international law committed or condoned by foreign governments.[187] While these issues are far from settled, at least one U.S. Circuit Court of Appeals has suggested "reckless disregard" is sufficient intent for liability under such ATS claims.[188] More recently, however, the United States Supreme Court has moved to limit the extraterritorial usage of ATS in cases like *Kiobel*; yet much of its scope, including application to human rights and related legal issues concerning online transnational activities, remains unresolved.[189]

Given the increasingly complex and central role intermediaries play in state surveillance and censorship – such as online service providers and gatekeepers – it is not difficult to imagine a U.S. company being sued for directly or indirectly assisting authoritarian regimes conducting online censorship, surveillance, or tracking that has led to human rights abuses. In fact, there are instances where this has already happened. Yahoo Inc., for example, famously settled an ATS legal action brought against it for intentionally or negligently assisting Chinese authorities in tracking down Chinese human rights activists and dissidents.[190] More recently, Cisco Systems was sued by a group of Chinese nationals and residents, including online dissident and writer Daobin Du, for supplying technology to the Chinese Government for use in its "Golden Shield" program for online censorship and

---

186 Alford, *supra* note 182, at 235–36.

187 *Id.* at 235.

188 Neil Conley, Comment, *The Chinese Communist Party's New Comrade: Yahoo's Collaboration with the Chinese Government in Jailing a Chinese Journalist and Yahoo's Possible Liability Under the Alien Torts Claim Act*, 111 PENN ST. L. REV. 171, 205 (2006).

189 *See generally* Anthony J. Colangelo, *The Alien Tort Statute and the Law of Nations in Kiobel and Beyond*, 44 GEO. J. INT'L L. 1329 (2013) (explaining how the scope of the ATS remains unclear following *Kiobel*).

190 Catherine Rampell, *Yahoo Settles with Chinese Families*, WASH. POST (Nov. 14, 2007), *available at* http://www.washingtonpost.com/wp-dyn/content/article/2007/11/13/AR2007111300885.html?hpid=topnews.

tracking.[191] Although the case was dismissed by a District Court in Maryland on preliminary legal and jurisdictional matters, its ruling on ATS has been strongly criticized.[192]

But what about organizations and individuals involved in censorship resistance activities? Do they have anything to worry about concerning these expanding legal liabilities? Internet censorship resistance activities are fraught with complicated international legal issues – including human rights – that create serious risks and dangers. Again, it is not difficult to envision a person suffering serious harms for being caught using a censorship resistant system or tool, when dealing with censorship regimes and security apparatus in countries like China or Iran. But if a legal claim was ever brought against an organization involved in developing or distributing censorship resistant tools, it would probably look like the infamous Haystack controversy – wherein developers greatly exaggerated the capabilities of a program allegedly designed to allow citizens in countries like Iran and China to safely circumvent Internet censorship and surveillance.[193] In such instances, it would not be a stretch to claim Haystack developers exhibited "reckless disregard"[194] and indirectly aided state authorities if an Iranian citizen was arrested or otherwise harmed for using the flawed Haystack tool.

Of course, there are other complex issues in such cases, and ATS case law continues to evolve and, as noted, is largely unresolved. At the very least, they complicate the regulatory

---

191 Cindy Cohn & Rainey Reitman, *Maryland Court Dismisses Landmark Case that Sought to Hold Cisco Responsible for Violating Human Rights,* ELEC. FRONTIER FOUND.: DEEPLINKS BLOG (Feb. 27, 2014), *available at* https://www.eff.org/deeplinks/2014/02/maryland-court-dismisses-landmark-case-sought-hold-cisco-responsible-violating; Rob Lever, *Cisco Cleared in Rights Case, as Tech Sector Watches*, DIGITAL J. (Nov. 13, 2007), http://digitaljournal.com/biz/business/cisco-cleared-in-rights-case-as-tech-sector-watches/article/373736.

192 Cohn & Reitman, *supra* note 191.

193 Evgeny Morozov, *More on Internet Intellectuals and the Haystack Affair*, FOREIGN POL'Y (Sept. 15, 2009), *available at* http://neteffect.foreignpolicy.com/posts/2010/09/14/more_on_internet_intellectuals_and_the_haystack_affair.

194 The "reckless disregard" standard for Alien Torts principles was endorsed by Justice Reinhardt in his concurring opinion in the Ninth Circuit's *Unocal II* decision: John Doe I v. Unocal Corp., 395 F.3d 932, 954–56 (9th Cir. 2002), *vacated, reh 'g en banc*, 395 F.3d 978 (9th Cir. 2003). *See* Conley, *supra* note 188, at 205–06 (considering the "reckless disregard" standard, and applying it to the Yahoo / Shi Tao case).

online space and cannot be ignored by either state or non-state actors – for better or for worse.

5.4. Network Neutrality, Encryption Rights, and the Economics of Privacy

Mass Internet surveillance remains a critical and growing threat to privacy and security. State signaled intelligence and electronic spying agencies are heavily investing in building mass surveillance capacity, including surveillance technologies and code breaking.[195] The significance of some recent revelations that the N.S.A. may have the ability to circumvent most encrypted messages[196] and are building "quantum" computers to break most cryptographic methods[197] has led to an important debate about privacy and the usefulness of popular encryption standards and methods.[198] On one side are experts like Adir Shamir, considered to be the "godfather" of encryption, who believes that we are in a "post-crypto world" and need to rethink security and privacy measures.[199] On the other side are experts such as Bruce Schneier who acknowledge powerful state capabilities and the shortcomings of encryption methods, but who still believes it is essential for ensuring security and privacy.[200] At a minimum, there may be

---

195 *See* Ball, *supra* note 1.

196 *See* Perlroth et al., *supra* note 1; Rich & Gellman, *supra* note 1.

197 Rich & Gellman, *supra* note 1.

198 *See* Andy Green, *Cryptography May Not Be Dead, but It Is on Life Support*, VARONIS BLOG (Jan. 21, 2014), http://blog.varonis.com/cryptography-may-dead-life-support/ ("Over the last year, cryptography and data security have been completely shaken by malware, and specifically advanced persistent threats or APTs, leading some to say or at least imply that cryptography is dead.").

199 John Leyden, *Prepare for 'Post-Crypto World', Warns Godfather of Encryption*, THE REGISTER (Mar. 1, 2013, 12:37 PM); *see* Kim Nursall, *Cicada 3301, Cryptography and the Quest for Anonymity*, TORONTO STAR (Jan. 3, 2014, 10:21 AM), http://www.thestar.com/entertainment/2014/01/03/cicada_3301_cryptography_and_the_quest_for_anonymity.html (quoting "a 25-year-old computer science student from Alberta . . . under the username Noxpopuli . . . [as saying,] "'You see a lot of the big names in (the field) talking about how cryptography is dead . . .'").

200 *See, e.g.*, Bruce Schneier, *NSA Surveillance: A Guide to Staying Secure*, THE GUARDIAN (Sept. 6, 2013, 9:09 AM), http://www.theguardian.com/world/2013/sep/05/nsa-how-to-remain-secure-surveillance; Bruce Schneier, *The NSA is Breaking Most Encryption on the Internet*, SCHNEIER ON SEC. (Sept. 5, 2013, 2:46 PM), https://www.schneier.com/blog/archives/2013/09/the_nsa_is_brea.html.

some insightful information gained from our case studies and telegraph discussions, and interesting legal or policy developments.

To begin with, courts tackling new cyber-security and related measures can return to the Telegraph Convention for guidance. Fifteen years after *Bernstein v. U.S. Justice Department*[201] forced the U.S. Government to scale back its export regulations on encryption technologies, similar privacy technology regulations may soon return under the guise of federal controls on "cyber-weapons" or cyber tools that could be used for "criminal, terrorist, or military activities."[202] Certainly, anonymizing tools that use encryption could fall into the National Defense Authorization Act's broad definition. If so, a broader constitutional right to use privacy or secrecy enhancing technologies may be required, or at least one that elaborates the Ninth Circuit's ruling in *Bernstein* further. On this count, the 1875 Telegraph Convention's innovative and express right to use secret language and code in telecommunications – as well as a policy preventing states from interfering with such transmissions – offers some historical, conceptual, and international legal precedential basis for such a right or interest.

Moreover, telegraph surveillance also provides some guidance on the "economics" of privacy and security today. Pervasive online surveillance capabilities demonstrated by state agencies like the N.S.A. have arguably now rendered Internet communications very much akin to telegraph communications in the late 1800s. At that time, Britain and a handful of other world powers owned

---

201 Bernstein v. U.S. Dep't of Justice, 176 F.3d 1132 (9th Cir. 1999), *vacated*, 192 F.3d 1308 (9th Cir. 1999) (holding that regulations preventing mathematician from distributing encryption software violated the First Amendment).

202 *See, e.g.*, National Defense Authorization Act for Fiscal Year 2014, Pub. L. No. 113-66, § 940(a)–(c), 127 Stat. 672, 837 (2013) (regulating the proliferation of cyber weapons and providing mechanisms for the military to develop cyber attack capabilities); *US Defense Budget to Both Regulate and Proliferate Cyber Weapons*, TRIPWIRE: THE STATE OF SEC. (Jan. 6, 2014), http://www.tripwire.com/state-of-security/top-security-stories/us-defense-budget-regulate-proliferate-cyber-weapons/ (commenting on the National Defense Authorization Act for Fiscal Year 2014); James Gorelick et al., *United States: Support Continues to Build for New Export Controls on Cyber Monitoring Technologies*, MONDAQ (Dec. 16, 2013), http://www.mondaq.com/unitedstates/x/281262/Export+controls+Trade+Investment+Sanctions/Support+Continues+to+Build+for+New+Export+Controls+on+Cyber+Monitoring+Technologies (outlining the sources of support for export controls for Internet Protocol network surveillance systems and equipment).

much of the telegraph system. Through that infrastructure, they conducted telegraph surveillance. Those sending an international telegram in plain language knew the message would pass by countless sets of eyes and hands at various cable stations around the world, wherein telegraph operators worked and re-routed cables. Those operators, working as "censors" for the British or other state governments, could easily intercept or steal important communications along the way.[203] That reality led, as noted, to widespread use of secret languages, codes, and other forms of "encryption" methods, both by companies and states to ensure secrecy in telegram communications. Of course, very much like today, for states heavily invested in cryptography and surveillance infrastructure, particularly Britain during World War I, mass surveillance still remained very costly and difficult – particularly code-breaking.[204] Even when governments prohibited encrypted communications during war, surveillance remained difficult due to the complex challenge of dealing with a "mass of telegraph messages."[205] The economics of telegraph surveillance meant it was never targeted "en mass" but focused on "specific targets."[206]

These historical insights encapsulate Schneier's argument about the use of encryption today. While the N.S.A. and state signal intelligence agencies have enormous capabilities, "they are not magical" and the best defense is "to make surveillance of us as expensive as possible."[207] This is the economics of privacy and mass surveillance. If a user is a target of the N.S.A., there are very few ways to avoid compromise in the face of an advanced persistent threat. However, just as the economics of privacy for the telegraph meant that use of codes and ciphers could often ensure an important measure of privacy, so too, for the vast majority of

---

203 Hills, *supra* note 44, at 198 (describing how the British government adopted procedures to control transnational communications in the event of war).

204 DOLLAR & GUNDERSON, *supra* note 61, at 853 ("*Much of this work of deciphering messages (1914–1918) was laborious and time consuming, still based largely upon frequency analysis*."); NICKLES, *supra* note 61, at 181 (discussing a story whereby U.S. State Department officials found it time consuming and difficult to decode their own coded cables).

205 Hills, *supra* note 44, at 197, 201 (noting that effective censorship likely required discrimination that targeted messages that were specifically likely to yield beneficial information).

206 *Id*.

207 Schneier, *NSA Surveillance*, *supra* note 200 (detailing the limitations of the NSA's surveillance program and suggesting that basic encryption methods can frustrate monitoring attempts).

Internet users, incorporating basic security measures and encryption use can ensure privacy and security even today. The more expensive mass surveillance is, the safer we are. Indeed, recent research suggests that the cheapening cost of mass surveillance, compared to earlier times, may be the greatest threat to privacy and liberty concerns.[208]

This raises another important question – the importance of legally promoting network neutrality to protect privacy and security. One of the more contentious and important regulatory debates concerning the Internet today is focused on "network neutrality" – put simply: whether Internet and telecommunication providers should be legally obliged to treat all Internet traffic and data the same. Thus, under a net neutral regime there can be no "broadband discrimination" or other actions to treat some traffic different from others.[209] Though usually related to broader regulatory and communication policy, our case study in telegraph surveillance provides insights into its importance for what I have been referring to as the "economics of privacy." An important legal measure that helped ensure privacy through telegram communications was the 1875 Telegraph Convention's requirement that states allow any "encrypted" telegraph transmissions through their territory (and if they did not, they had to notify the state of origins).[210] This rudimentary telegraph communication network neutrality requirement, in normal times, rendered surveillance or censorship of encrypted telegrams much more impractical, raising costs and the legal stakes. Today, with

---

[208] Kevin S. Bankston & Ashkan Soltani, *Tiny Constables and the Cost of Surveillance: Making Cents Out of U.S. v. Jones*, 123 YALE L.J. 335 (2014) (reviewing the economic cost of implementing various forms of surveillance and identifying methods that make long term monitoring relatively cheap); *see generally* Ian Brown, *The Economics of Privacy, Data Protection and Surveillance*, *in* HANDBOOK ON THE ECONOMICS OF THE INTERNET (M. Latzer & J. M. Bauer eds., 2015) ("Law enforcement and intelligence agencies are intensive users of surveillance technologies and data gathered by third parties, especially as the technologies to perform such surveillance become ever cheaper") (citation omitted).

[209] *See generally* Tim Wu & Christopher S. Yoo, *Keeping the Internet Neutral?: Tim Wu and Christopher Yoo Debate*, 59 FED. COMM. L.J. 575 (2007) (debating whether deviations from network neutrality would necessarily harm consumers and innovation); Tim Wu, *Network Neutrality, Broadband Discrimination*, 2 J. TELECOMM. & HIGH TECH. L. 141 (2003).

[210] International Telegraph Convention, *supra* note 39, art. VI, VIII. I use "encrypted" here in quotations to note that many of the secret codes and languages used would not, by modern standards, constitute a proper cryptographic method.

reports of ISPs throttling, blocking, or discriminating against encrypted Internet traffic[211] – in clear violation of network neutrality principles – the push to preserve such neutrality becomes that much more important to the economics of surveillance and our privacy rights. Again, the more costly the surveillance is for the watchers, the safer regular users will be from mass forms of surveillance.

5.5. Other Cooperative and Effective Measures: Legal, Institutional, Political

5.5.1. Alternative Regulatory Role for International Institutions

As noted, one of the themes argued here based on the case studies is that global telecommunications were better protected from state censorship, disruption, and control by more cooperative endeavors among the many states. The case studies offer some concrete ideas for similar cooperative approaches today that might either forge a different path from pure information conflict and control, or, at the very least, attenuate its impact on the Internet and its reach.

First, that in the years ahead, information conflicts concerning the Internet will be fought in "cyberspace" – likely through "cyberwarfare" – but also through international institutions. The Cold War information conflicts were played out not only in battlefields and proxy wars, but also within and between international institutions. We may be seeing this already in relation to the Internet from recent controversies focused on the ITU. In light of this, those concerned with the fate of Internet freedom such as states, organizations, and individuals, would do well to not withdraw from these organizations, but to continue to advocate for the free flow of information.

Second, a purely negative vision for international law and institutions will not do. Much of the discourse offered by Internet

---

[211] April Glaser, *Net Neutrality Isn't Totally Lost: Here's How the FCC Can Test for ISP Bad Behavior*, SLATE (Jan. 31, 2014, 10:02 AM), http://www.slate.com/blogs/future_tense/2014/01/31/net_neutrality_isn_t_totally_lost_the_fcc_can_test_for_isp_bad_behavior.html ("In recent years we've seen dozens of Internet providers in the United States and around the world act in non-neutral ways. In 2007, for example, Comcast was caught interfering with its customers' use of Bit Torrent and other peer-to-peer file sharing. We witnessed a major Canadian ISP slow down all encrypted file transfers . . .").

activists in opposition to the ITU and the WCIT potential "takeover" of the Internet was simply that the ITU should keep its hands off and go away. But the ITU is unlikely to go anywhere. Moreover, if we are to believe the recent Congressional testimony of Federal Communications Commissioner Robert McDowell, the ITU has committed to reinventing itself in relation to the Internet, just as it had for technologies before it, such as the telegraph, telephone, radio, and communications satellite.[212] Withdrawing from international institutions, or failing to offer a role for them to play, leaves those same institutions and their future direction open to states like China, Russia, or Iran, whose aim to control and censor the Internet are clear.

So, what might a positive role look like? The ITU's Cold War radio jamming monitor offers one possible vision. In some ways, the radio jamming monitoring program, implemented in the 1980s, was an earlier version of more contemporary efforts to map and track Internet censorship around the world that is carried out by non-governmental organizations such as the OpenNet Initiative and Herdict. The success of the IFRB – even if the program was short lived – provides additional insights into its program's great value and potential influence. Of course, the difference between such non-governmental efforts and an ITU-led Internet censorship monitor is that the latter would, like its earlier radio incarnation, have a much deeper pool of resources to draw on for technical implementation and would also have the UN's institutional reach for large scale coordination and exposure, adding even greater reputational costs to the dark art of Internet censorship.

5.5.2. Influencing the "Middle"

Such an Internet censorship-monitoring program would be

---

212 *Fighting for Internet Freedom: Dubai and Beyond, Joint Subcommittee Hearing Before the U.S. House of Representatives, Committee on Energy and Commerce, Subcommittee on Communications and Technology, Committee on Foreign Affairs, Subcommittee on Terrorism, Nonproliferation, and Trade, Committee on Foreign Affairs, Subcommittee on Africa, Global Health, Global Human Rights, and International Organizations* (2013) (statement of Robert M. McDowell, Commissioner, Federal Communications Commission), *available at* http://docs.house.gov/meetings/IF/IF16/20130205/100221/HHRG-113-IF16-Wstate-McDowellR-20130205.pdf (outlining newly acquired policing powers of the ITU over the internet).

beneficial, not just in providing greater knowledge and insight about global censorship trends, but also in influencing the "middle." That is, rather than focusing on high profile (and commonly cited) countries like China and Iran that are committed to broad and sophisticated Internet censorship, the program would focus instead on the broader middle – the range of countries that engage in some level of Internet filtering or censorship but that may be more responsive to bad press or international exposure because they are more concerned about their reputation and the economic costs of censorship. During the Cold War, the Soviet Union was unrelenting both in its resolve and technical capacity to jam Western radio broadcasts and no amount of international exposure or condemnation deterred it from that path. But, as noted in our study, less wealthy countries were more easily swayed by international exposure through ITU monitoring. This was likely due to a range of factors such as the costs involved in radio jamming, sensitivity to international reputation, or simply wishing to avoid stepping into the middle of an ongoing dispute between superpowers – the United States and the Soviet Union.

5.5.3. Avoiding Cold War Analogies

Finally, it should be said that among certain legal and public policy circles, and certainly within the national security establishment, there is a growing trend to describe and address the challenges of Internet cyber-security matters through the lens of the Cold War. While there are certainly descriptive and analytical reasons for drawing on Cold War experiences to understand current developments like the "militarization" of cyberspace,[213] these case studies suggest that adopting Cold War analogies may do more harm than good to Internet censorship and surveillance resistance. Historically, international legal protections for free and open global communications have been more robust in times of peace and weakest in times of war.

This was the case with the Telegraph Conventions, which all provided relatively effective protection against telegram blocking

---

[213] *See generally* Nye, *supra* note 1. *See also* Ronald Deibert, *Militarizing Cyberspace*, MIT TECH. REV. (June 22, 2010), *available at* http://www.technologyreview.com/computing/25570/ (expounding upon the power dynamics of cyberspace).

and cable cutting among peaceful countries but proved inadequate in dealing with nations at war. Similarly, global radio programming was never more free and unencumbered by censorship and other jamming activities than during the peaceful years after the Second World War, before the Cold War was in full swing. State and national security officials eager to approach Internet and cyber-security issues with Cold War strategies have self-interested reasons for doing so – free and open Internet communications are easier to limit and control at war. Both the history and current challenges concerning Internet censorship are complex; simple parallels to the Cold War, at the very least, gloss over those complexities.

6. CONCLUSION

The aim of this work is neither to establish that global telecommunication technologies follow a predetermined regulatory path nor to expound the precise state of international telecommunications law. Rather, the point is to promote a more informed debate about current and historical regulatory challenges posed by telecommunications technology through the exploration of three case studies – involving influential and, in their time, predominant telecommunications technologies – and extrapolate theoretical, legal, or policy insights therefrom. Part of that exploration has identified some interesting and noteworthy regulatory patterns. For instance, the "cycles" of global telecommunication censorship and surveillance, and the insight that more cooperative approaches have led to more effective regulatory outcomes in protecting global telecommunications from disruption, censorship, or control. However, to be clear, the analysis also suggests the "cycles" or patterns are neither obviously uniform nor congruent, inevitable, or universal; but they are useful and worthy of further study. These insights, and others outlined here, hopefully provide some additional foundation and framework to tackle challenges posed by the evolving forms of Internet control, censorship, and surveillance today. At the very least, analysts, lawyers, and policymakers would do well to not ignore these parallels. The internet's regulatory story is still unfolding, but at least these cases on global telecommunications technologies and their censorship, surveillance, and disruption

provide some basic ways to improve our chances to avoid or resist sustained information conflict, control, and, ultimately, paralysis.