University of Chicago Legal Forum

Volume 2001 | Issue 1 Article 4

The Internet and the Legitimacy of Remote Cross-Border Searches

Jack L. Goldsmith
Jack.Goldsmith@chicagounbound.edu

The Internet and the Legitimacy of Remote Cross-Border Searches

Jack L. Goldsmith[†]

In the fall of 2000, the FBI learned that hackers were breaking into the computer networks of banks, internet service providers, and other firms in the United States. From computers in the United States, the FBI traced the source of the hack to servers in Russia. The FBI tried, and failed, to secure Russian assistance in monitoring and redressing the criminal activity. It decided to act unilaterally. After obtaining a search warrant in the United States, it used a "sniffer" keystroke recording program to learn the hackers' usernames and passwords. It then used this information to download incriminating information from the hackers' computers in Russia.[1]

The FBI's actions are known as *remote cross-border searches and seizures*. Searches and seizures of this sort are an important tool in fighting cybercrime. Cross-border theft, hacks, worms, and denial-of-service attacks cause significant damage to computer systems in the United States. To redress such crimes, it is crucial to identify the computer source of the criminal activity and seize (or at least freeze) information relevant to the crime before records of it are erased. The demand for information about computer activity abroad will undoubtedly increase significantly in the wake of the September 11, 2001 terrorist attack on the United States.

One way for a nation to get information on a computer in another nation is to cooperate with enforcement officials in the source nation. The problem is that such cooperation is often difficult. Sometimes the source-country government lacks legal authority to seize and freeze computer information within its bor-

---

† Professor of Law, University of Chicago Law School. Thanks to Neal Katyal, Adrian Vermeule, Eric Posner, Tracey Meares, and Kal Raustiala for helpful comments, and Dave Scott and Josh Walker for research assistance.

[1] See Robert Lemos, *Lawyers Slam FBI 'Hack,'* ZDNet News (May 1, 2001), available online at <http://www.zdnet.com/zdnn/stories/news/0,4586,5082126,00.html> (visited July 6, 2001) [on file with U Chi Legal F]. See also Allison Linn, *FBI's Elaborate Hacker Sting Pays Off: High-Tech Gambit Nets 2 Russians*, Chi Trib 20 (May 10, 2001).

ders. Sometimes it lacks the technological capacity. Sometimes the enforcement machinery in the source country will simply take too long, because evidence of the crime can quickly be destroyed or anonymized. And sometimes, as in the opening example, the source-country government simply fails to cooperate. For these and other reasons, officials in the target country might take matters into their own hands. Sitting at their computers, they might trace the origins of the cybercrime, and explore, freeze, and store relevant data located on computers abroad.

Many believe that such cross-border searches and seizures on computer networks by enforcement officials in one country violate the territorial sovereignty of the country where the data is located.[2] This view appears to find support in the international law prohibitions on extraterritorial enforcement jurisdiction. The Restatement (Third) of Foreign Relations Law states these limits as follows: "It is universally recognized, as a corollary of state sovereignty, that officials in one state may not exercise their functions in the territory of another state without the latter's consent."[3] The Restatement adds that one state's law enforcement officials "can engage in criminal investigation in [another] state *only with* that state's consent."[4]

This essay argues that remote cross-border searches and seizures are consistent with international principles of enforcement jurisdiction.[5] It does not argue that there will be no limits on such searches, but rather that such limits are not deducible from norms of territorialism. Instead, the limits will emerge from a messy process of cross-border search and retaliation, as nations adjust themselves to the changed circumstances of a new technology. Along the way, the essay hopes to shed light on the relationship between technological change and the evolution of our jurisdictional concepts.

A caveat is in order at the outset. In arguing that remote cross-border searches can be legal from a jurisdictional perspec-

---

[2] See, for example, Stephen Wilske and Teresa Schiller, *International Jurisdiction in Cyberspace: Which States May Regulate the Internet?*, 50 Fed Commun L J 117, 174 (1997); Henry H. Perritt, Jr., *Jurisdiction in Cyberspace*, 41 Vill L Rev 1, 82–83 (1996). See also Lemos, *Lawyers Slam FBI 'Hack,'* ZDNet News (cited in note 1); Linn, *FBI's Elaborate Hacker Sting*, Chi Trib at 20 (cited in note 1).

[3] Restatement (Third) of the Foreign Relations Law § 432 comment b (1987).

[4] Id (emphasis added).

[5] Many other elements of international law might be relevant here, including, potentially, the U.N. Charter's prohibition on the use of force except in self-defense. Charter of the United Nations, Arts 2, 51, 59 Stat 1031, Treaty Ser No 993 (1945). But in this symposium devoted to jurisdiction, I will focus on international law of jurisdiction.

tive, I do not (directly) address the many possible "substantive" reasons why the exercise of this jurisdiction may be problematic. Remote cross-border searches might be justified on jurisdictional grounds but unjustified from the perspective of privacy or free speech rights. These latter issues are important, and indeed they might even be relevant to a jurisdictional analysis, as discussed below. But a full analysis of individual rights restrictions on remote cross-border searches is beyond the scope of this paper.[6] I shall instead analyze the more fundamental jurisdictional issues that are the subject of this symposium.

I. THE PRACTICAL NECESSITY OF REMOTE CROSS-BORDER SEARCHES

The term "cybercrime" subsumes many different activities. I focus here on "unauthorized access" crimes and "unauthorized disruption" crimes (viruses, worms, logic bombs, trojan horses, distributed denial of service attacks, etc.)[7] These are crimes committed by computers via the internet that illegally access or harm files and programs on other computers. I am interested in such crimes when they originate on computers in one country and illegally access or cause damage to computers in another country. The Russian hackers discussed at the outset provide an example of unauthorized cross-border access. An example of unauthorized cross-border disruption is the "I Love You" worm that originated on a computer in the Philippines and caused over eleven billion dollars in losses in the United States.[8]

Cybercrimes with these characteristics are difficult for the nation where the crime occurs to regulate. As a general matter, nations exercise regulatory control over internet transmissions from abroad by regulating its local connections—assets, end-users, internet intermediaries, and hardware and software within their territories.[9] These forms of territorial regulation tend not to

---

[6] See, for example, *United States v Verdugo-Urquidez*, 494 US 259 (1990) (holding that the Fourth Amendment does not apply to searches and seizures of property owned by non-resident aliens located in foreign countries).

[7] For an overview of these types of cybercrimes, see Neil Kumar Katyal, *Criminal Law in Cyberspace*, 149 U Pa L Rev 1003, 1013–27 (2001).

[8] *'Love Bug' Virus Case Dropped in Philippines; No Legal Grounds for Trial of Student*, Wash Post A12 (Aug 22, 2000).

[9] For an elaboration of these truncated points, see Jack L. Goldsmith, *Against Cyberanarchy*, 65 U Chi L Rev 1199, 1221–24 (1998); Jack L. Goldsmith, *The Internet and the Abiding Significance of Territorial Sovereignty*, 5 Ind J Global Legal Stud 475, 481–83 (1998).

work well, however, with respect to cross-border crimes.[10] Because such crimes are (usually) discrete events, it is hard for local internet intermediaries to identify and screen out the pertinent cross-border data flows at any cost short of ex ante examination of every internet communication. Moreover, there is a special need in this context to secure evidence of the crime immediately. These crimes can be initiated in advance of detection. Pseudonymity is relatively easy to achieve in the commission of these crimes. And perhaps most importantly, evidence of the crime can be destroyed relatively quickly.[11]

For these reasons, enforcement authorities must address cross-border crimes quickly at their source. One way to do this is through cooperation between the nation subject to the attack and the nation (or nations) from which, or through which, the attack occurs. Officials in the originating state(s) can assist officials in the target state in identifying, freezing, and retrieving evidence related to the crime, and in apprehending the author of the crime and either bringing her to justice in the originating state or extraditing her to the target state for prosecution.

This, in a nutshell, is the strategy of the Council of Europe Cybercrime Convention.[12] In addition to harmonizing domestic definitions of cybercrime,[13] the Convention aims to enhance fast and effective international cooperation in preventing it. The Convention requires each nation to enact laws authorizing expedited searches, seizures, and preservations of computer data *within the territory*.[14] It also provides for rapid enforcement assistance. For example, the Convention contemplates that nations where the crime originates will, at the request of the nation where the crime causes damage, preserve and disclose stored computer data.[15] It also contemplates that each treaty signatory will establish a round-the-clock "point of contact" to ensure immediate assistance for the purposes of cross-border information requests.[16]

---

[10] I am assuming here that for the foreseeable future, purely defensive mechanisms will be an inadequate response to cross-border cybercrimes.

[11] See, for example, Katyal, 149 U Pa L Rev at 1074 (cited in note 7).

[12] Council of Europe Committee of Ministers, 109th Sess, Convention on Cyber-Crime (adopted Nov 8, 2001), available online at <http://conventions.coe.int/Treaty/EN/projets/FinalCybercrime.htm> (visited Nov 14, 2001) [on file with U Chi Legal F].

[13] See id at Arts 2–13.

[14] See id at Arts 16–21. The territorial limits on these activities is made explicit in Articles 19 and 20 (which concern the search, seizure, and collection of data), by the jurisdictional provisions in Article 23(a), and by Article 32, which limits cross-border searches to publicly available data or private data only with consent.

[15] See id at Arts 29–34.

[16] Convention on Cyber-Crime at Art 35 (cited in note 12).

Critics have attacked the European Cyber-Crime Convention for, among many other reasons, threatening civil liberties and imposing exorbitant obligations on internet service providers and other intermediaries.[17] And yet it seems clear that the Convention as currently drafted will not adequately redress the problem of cross-border unauthorized disruption crimes. It will take years to finalize the treaty and secure its ratification and domestic implementation. Effective responses are needed in the interim. Once ratified, the cooperative mechanisms established by the Convention will only be effective if there is universal consent to the treaty. The Convention will have little influence on crimes committed from safe-haven nations that do not ratify it.[18] This suggests that for the Convention to work, State parties will need to impose significant collateral sanctions on nations that fail to ratify, implement, or enforce it.

Most important for present purposes, the Convention does not authorize remote cross-border searches, even in cases of emergency or hot pursuit.[19] Assuming that the Convention eventually comes into force, it requires a nation pursuing a cybercriminal to consult with local officials before seizing, storing, and freezing data on computers located in their countries.[20] Even with the contemplated round-the-clock consultation and mutual assistance machinery, this extra and unwieldy step will give cybercriminals precious time to cover their tracks. As the FBI's counter-hack in the opening example suggests, effective enforcement of cybercrime will sometimes demand unilateral remote cross-border searches and seizures.

---

[17] See Global Internet Liberty Campaign, Member Letter to Council of Europe Secretary General Walter Schwimmer and COE Committee of Experts on Cyber Crime (Dec 12, 2000), available online at <http://www.gilc.org/privacy/coe-letter-1200.html> (visited Oct 25, 2001) [on file with U Chi Legal F]; Patti Waldmeir, *Dark Side of Cybercrime Fight: An International Treaty on Law Enforcement for the Web Poses Unsettling Questions About Civil Liberties*, Fin Times, Inside Track 17 (May 10, 2001); Paul Meller, *ISP's join to cry foul over pending European cybercrime rules*, InfoWorld, Enterprise Networking 76c (March 26, 2001).

[18] At the margin it might influence the travel plans of known cyber-criminals, who will face the possibility of being arrested and extradited if they travel from a safe haven to a signatory country.

[19] According to Guy de Val, Director-General for Legal Affairs for the Council of Europe, the Convention "does not provide for actual cross-border investigations, nor cross-border searches, 'because the states which negotiated the draft were unable to agree on that point.'" See Europe Information Service, *Cybercrime: Community Accession to an International Convention*, European Report (Mar 21, 2001). See also Convention on Cyber-Crime (cited in note 12).

[20] See Convention on Cyber-Crime at Arts 29, 31 (cited in note 12).

II. THE LOGIC OF JURISDICTIONAL CHANGE

Are remote cross-border searches consistent with international law principles of jurisdiction? The Council of Europe's failure to authorize such searches presupposes that international law prohibits them in the absence of the consent of the nation in which the searched computers are located. But is this true? Does territorial sovereignty limit one nation's ability to search, seize, and freeze data related to a crime that is located in another country where the crime originates?

In answering this question, consider first *prescriptive jurisdiction*, which is the power of a nation to apply its laws.[21] It is uncontroversial that the United States has prescriptive jurisdiction to apply its criminal laws to, say, a crime that causes injury in the United States that is initiated from a computer abroad. International law principles of territorial sovereignty permit the United States to apply its laws to activities abroad that have substantial effects in the United States.[22]

The prohibition on seizing data abroad, however, is thought to be an issue of *enforcement jurisdiction*. Enforcement jurisdiction is a nation's power "to induce or compel compliance or to punish noncompliance with its laws or regulations."[23] As stated above, conventional wisdom says that a nation may not enforce its criminal laws outside of its territory.[24] But were FBI officials in our opening example *enforcing* laws *outside* the United States? The FBI action is ambiguous. On the one hand, the FBI gathered information physically located in another country. On the other hand, FBI officials never left their offices in the United States; they and their equipment remained at all times in the United States.

The concept of territorial sovereignty by itself cannot choose between these two conceptions of the remote cross-border seizure, and cannot by itself tell us whether the search was legitimate. "Territorial sovereignty" has never had a definitive content, has never been unchanging or sacrosanct, and has never prohibited all outside influences within a nation's borders.[25] Moreover, throughout history, nations have modified their views about the significance of territorial borders and the meaning of a "territo-

---

21 See Restatement (Third) of Foreign Relations Law § 401(a) (1987).

22 See id at § 402(1)(c); *Hartford Fire Insurance Co v California*, 509 US 764 (1993).

23 Restatement (Third) of Foreign Relations Law § 401(c) (1987).

24 See text accompanying notes 2–3.

25 See generally Stephen Krasner, *Sovereignty: Organized Hypocrisy* (Princeton 1999).

rial violation," in response to changed international circumstances, including changed technological circumstances. We thus must look to history and reason by analogy to see whether, and to what extent, cross-border searches are likely to become an accepted practice among nations.

Begin with some old and simple principles of jurisdiction. Joseph Story famously stated the classical principles of territorial sovereignty as follows. First, "every nation possesses an exclusive sovereignty and jurisdiction within its own territory."[26] Second,

> no state or nation can, by its laws, *directly* affect, or bind property out of its territory, or bind persons not resident therein .... This is a natural consequence of the first proposition; for it would be wholly incompatible with the equality and exclusiveness of the sovereignty of all nations, that any one nation should be at liberty to regulate either persons or things not within its own territory.[27]

The key word here is "directly." Even a territorialist like Story realized that through purely territorial exercises of power, one nation can *indirectly* regulate persons and property abroad.[28] Indirect regulation works because the regulating nation brings force to bear on persons and property within its territory, and this purely local force (or threat of force) can have effects on behavior abroad. If an offshore person or firm causes local harm from abroad, the local government can indirectly regulate the harmful foreign activity by threatening to seize the offshore firm's local assets. The United States is able to apply its securities laws, antitrust laws, and criminal laws to activities abroad because many offshore entities have a U.S. presence (assets, employees, debts, etc.) that the United States can threaten to seize in response to non-compliance with its regulations. The United States is not the only nation to exercise this power. The European Commission was able to block the proposed merger, approved by U.S. officials, of the U.S. companies General Electric and Honey-

---

[26] See Joseph Story, *Commentaries on the Conflict of Laws, Foreign and Domestic, in Regard to Contracts, Rights and Remedies, and Especially in Regard to Marriages, Divorces, Wills, Successions, and Judgments* § 18 at 19 (Little, Brown 2d ed 1841).

[27] Id at § 20 (emphasis added).

[28] Ulrich Huber, the sixteenth century Dutch scholar on whom Story relied, acknowledged the same point. See Ulrich Huber, *De Conflictu Legum Diversarum in Diversis Imperiis* (1689), excerpted and translated in Ernest G. Lorenzen, *Selected Articles on the Conflict of Laws* 163–66 (Yale 1947).

well International.[29] The Commission had leverage over these firms because the firms had extensive assets in Europe; the threat of force against these assets gave the Commission the power to halt the merger.

Nations have always exercised indirect extraterritorial regulation of this sort. They have always exercised territorial power in ways that changed behavior in other nations. Indeed, indirect extraterritorial regulation of this sort is inevitable in a world of decentralized lawmaking and trans-jurisdictional transactions. One nation's regulation of a cross-border transaction will always have consequences in other nations to which the transaction is connected.

What has changed in modern times is not indirect extraterritorial regulation per se, but rather the *scope* of indirect extraterritorial influence. Throughout modern history, the permissible scope of a nation's extraterritorial influence has expanded pursuant to the following inexorable logic. Technological and related exogenous changes lower the costs of cross-border communication and travel. These changes increase cross-border activity, and make it easier for activity originating in jurisdiction A to have effects (including harmful effects) in jurisdiction B. The government of B, responsible for protecting local interests, takes increasingly aggressive steps within its territory to redress these new local harms from A. These steps expand the indirect extraterritorial effect, in A, of B's purely territorial assertions of authority. The result is a change in our conception of what "territorial sovereignty" permits.

This in a nutshell is the logic and historical pattern of jurisdictional change. Note several important characteristics of this logic. First, changes in technology expand extraterritorial influence in both directions. Both the source nation and the target nation, acting within their territory (where "acting" includes permitting activity within the territory), have increasing influence abroad. Second, the influence of territorial power simultaneously expands and contracts, along different dimensions, through time. In the example above, A at first glance seems empowered by technological change, because activity within it (whether prohibited or authorized by A's government) increasingly has effects abroad. For the same reason, B initially seems weakened by technological change. But B fights back with its own in-state acts,

---

[29] See Edmund L. Andrews and Paul Meller, *Europe Ends Bid by G.E. for Honeywell*, NY Times C1 (July 4, 2001).

and these acts, in part facilitated by the technological change that has increased cross-border activity in the first place, has heightened extraterritorial effects in A. In both directions, technological change alters the extraterritorial influence of purely territorial action.[30]

To better understand these somewhat abstract points, and to see how they apply to remote cross-border searches, begin with personal jurisdiction. Like most exercises of jurisdiction, personal jurisdiction was once conceptualized in purely territorial terms. International law permitted states to assert personal jurisdiction only if a defendant was served within its territory, or if the defendant's property was attached within the territory.[31]

This regime came under pressure with the advent of technological innovations such as the automobile and the telephone, and related changes such as the rise of the multi-state corporation.[32] These developments made it easier for out-of-state actors to cause local harms while at the same time escaping territorial service of process. And this, in turn, enabled out-of-staters to avoid local personal jurisdiction and thus local responsibility for local harms. States refused to countenance these circumventions of local regulatory authority. They developed fictions that were nominally consistent with hermetic territorialism but that allowed them to expand their regulatory reach.[33] Eventually, the Supreme Court abandoned these fictions and held that federal due process allowed states to serve defendants with process out of state, and thus to establish personal jurisdiction over out-of-staters who caused local harms.[34] This change in due process law in effect expanded the authority of states over out-of-state activities. Similar trends took place on the international plane, for similar reasons.[35]

Now consider the regulation of international markets. Before World War II, international law prohibited nations from regulat-

---

[30] The stylized example in the last two paragraphs purposefully abstracted away from the complication of power asymmetries.

[31] See *Pennoyer v Neff*, 95 US 714, 730 (1877) (invoking law of nations).

[32] See *Hanson v Denckla*, 357 US 235, 251, 260 (1958); *McGee v International Life Insurance Co*, 355 US 220, 222–23 (1957); Philip B. Kurland, *The Supreme Court, the Due Process Clause, and the In Personam Jurisdiction of State Courts: From* Pennoyer *to* Denckla*: A Review*, 25 U Chi L Rev 569, 573 (1958).

[33] See *Henry L. Doherty & Co v Goodman*, 294 US 623 (1935); *Hess v Pawloski*, 274 US 352 (1927); *Kane v New Jersey*, 242 US 160 (1916).

[34] See, for example, *Burger King Corp v Rudzewicz*, 471 US 462 (1985); *International Shoe Co v Washington*, 326 US 310 (1945).

[35] See generally Friedrich Juenger, *Federalism: Judicial Jurisdiction in the United States and in the European Communities: A Comparison*, 82 Mich L Rev 1195 (1984).

ing activities in foreign markets.[36] As technological change following World War II led to more interdependent international markets, and as the regulatory state burgeoned, the United States began to apply its antitrust and securities laws to regulate activities abroad.[37] The United States viewed such extraterritorial regulation as necessary to protect local markets that, in an increasingly integrated global economy, could more easily be affected by activities abroad. Ultimately, the United States was successful in asserting its regulatory authority in this way because it could threaten the local assets of firms engaging in harmful offshore activity. Other countries originally greeted U.S. extraterritorial regulation with indignant protest, arguing that the United States was illegitimately influencing activity outside its borders.[38] But today the "effects" test for extraterritorial regulation is well established around the world.[39]

The lesson here, once again, is that exogenous communication and technological changes increased local harms from abroad, and aggressive regulatory responses to these harms both expanded indirect extraterritorial influence and altered the accepted norms of territorial sovereignty. Just as in the personal jurisdiction example, what nations once viewed as impermissibly "extraterritorial" came to be viewed as a legitimate territorial action justified by the need to redress the harmful local effects of offshore activities.

The extraterritorial economic regulations examples involve prescriptive rather than enforcement jurisdiction. But this distinction is misleading.[40] The only reason that extraterritorial pre-

---

[36] An example of the strictly territorial application of regulatory authority in the United States is *American Banana Co v United Fruit Co*, 213 US 347, 359 (1909) (holding that U.S. antitrust law has no extraterritorial application).

[37] See, for example, *Schoenbaum v Firstbrook*, 405 F2d 200, 208 (2d Cir 1968) (applying U.S. securities law to foreign transactions with local effects); *United States v Aluminum Co of America*, 148 F2d 416, 424 (2d Cir 1945) (applying U.S. antitrust law to offshore activity with local effects).

[38] See Gary Born and David Westin, *International Civil Litigation in United States Courts: Commentary and Materials* 600–03 (Kluwer 2d ed 1992).

[39] A good example is the European Commission's actions mentioned above at note 29. More broadly, the Europeans have embraced an effects test for extraterritorial regulation very similar to the United States approach Europe used to abhor. See Roger P. Alford, *The Extraterritorial Application of Antitrust Laws: The United States and European Community Approaches*, 33 Va J Intl L 1 (1992).

[40] It is perhaps worth noting in this regard that the distinction between prescriptive and enforcement jurisdiction, like many other distinctions in international law, is an invention of the American Law Institute's Restatement project. One does not find mention of the distinction before the 1965 Restatement, or in non-U.S. discussions of international law.

scriptive authority is efficacious in these regulatory contexts is that territorial enforcement authority provided leverage over foreign activity. Acting purely within its territory, the United States was able to bring about change abroad, and thus to indirectly enforce its laws abroad to regulate activity there.

Now consider an example that clearly involves enforcement jurisdiction and is directly analogous to remote cross-border searches on the internet. At one time, the United States refused to order firms with a U.S. presence to disclose documents abroad if doing so violated foreign bank secrecy law.[41] These courts reasoned that such disclosure orders exceeded the limits of enforcement jurisdiction and were inconsistent with international comity. U.S. courts began to change their tune, however, in the face of technological changes that made it easier to avoid liability for local harms by transferring and hiding illegal funds and transactions in banks and institutions abroad.[42] Many U.S. courts have ordered a U.S. branch office to disclose documents in a parent or branch abroad, even if doing so violates foreign law.[43] Such orders are obeyed because of the court's credible threat to seize or fine local assets. These judicial orders clearly have the direct and immediate effect of revealing information from abroad, even though the court's power technically extends only to its territorial border.

We can now generalize about the relationship between technological change and jurisdictional scope. Technological developments in communication and transportation increase cross-border activity between nations. This has made it cheaper, and thus easier, for out-of-state actors to cause local harm from abroad. If the local government cannot secure adequate cooperation from foreign authorities to fully redress such harms, it will take unilateral steps to address them. Governments tend not to send police forces into other nations without permission—though they sometimes do.[44] Instead, governments usually take steps *within their territories* to indirectly alter offensive behavior abroad. These in-

---

[41] See, for example, *Application of Chase Manhattan Bank*, 297 F2d 611, 612–13 (2d Cir 1962); *Ings v Ferguson*, 282 F2d 149, 152–53 (2d Cir 1960); *First National City Bank of New York v IRS*, 271 F2d 616, 619 (2d Cir 1959).

[42] See C. Todd Jones, *Compulsion Over Comity: The United States' Assault on Foreign Bank Secrecy*, 12 Nw J Intl L & Bus 454 (1992).

[43] See *In re Grand Jury Proceedings Bank of Nova Scotia*, 740 F2d 817, 832–33 (11th Cir 1984); *United States v Bank of Nova Scotia*, 691 F2d 1384, 1390–91 (11th Cir 1982); *SEC v Banca Della Svizzera Italiana*, 92 FRD 111, 118–19 (S D NY 1981). See also Jones, 12 Nw J Intl L & Bus at 464–71, 488–99, 502–07 (cited in note 42).

[44] Consider, for example, NATO's recent bombing of Kosovo, the first George Bush's invasion of Panama, and the Russian invasion of Chechnya.

creasingly aggressive steps are necessary to redress increasing local harms from abroad. "Law" follows behavior here, resulting in an altered conception of what "territorial sovereignty" requires and an expansion in permissible "extraterritorial" activity.[45]

To this generalization we can add a different but related one that also sheds light on cross-border internet searches. Nations have long gathered information located in other nations without physically entering the territory of those nations. For hundreds of years, ships on the high seas have used binoculars, spyglasses, telescopes, and periscopes to learn what's going on inside a country. Balloon aerial surveillance dates to the French revolution,[46] and was frequently employed in the American Civil War.[47] Airplane reconnaissance dates to the 1911 Italo-Turkish War, and remains an important means of cross-border surveillance.[48] During the last fifty years the United States has made tens of thousands of flights in international air space to gather reconnaissance information inside other countries.[49] At least half a dozen countries (not to mention scores of private firms) employ orbital reconnaissance satellites to monitor activities within other countries. The most sophisticated of these satellites can distinguish objects that are as small as six inches, and digital data provided by these satellites can be further manipulated by local computers to provide even more detailed three-dimensional images.[50]

So once again, we see technological innovation making it easier and easier for one nation to gather information in another nation without physically crossing borders. Norms of "territorial sovereignty" have never precluded such offshore espionage. There is a simple reason for this: Nations are interested in what goes on inside other nations, and there is no across-the-board, cost-effective way to stop such spying. We do, of course, see a technological arms race: The nation where the information is located

---

[45] For a general account of this method of international law development, see Jack L. Goldsmith and Eric A. Posner, *A Theory of Customary International Law*, 66 U Chi L Rev 1113, 1120–39 (1999).

[46] See General Carl Spaatz, *Evolution of Air Power: Our Urgent Need for an Air Force Second to None*, 11 Milit Affairs 2, 3 (Spring 1947).

[47] For a general discussion, see Edwin C. Fishel, *The Secret War for the Union: The Untold Story of Military Intelligence in the Civil War* (Houghton, Mifflin 1996).

[48] See Jeffrey T. Richelson, *A Century of Spies: Intelligence in the Twentieth Century* 17 (Oxford 1995).

[49] Christopher Drew, *Collision with China: Intelligence Gathering*, NY Times A6 (Apr 14, 2001).

[50] See Robert Windrem, *Spy Satellites Enter New Dimension*, MSNBC (Aug 8, 1998), available online at <http://www.msnbc.com/news/185953.asp?cp1=1> (visited July 7, 2001) [on file with U Chi Legal F].

takes steps within its territory to block or counteract the offshore surveillance, and the nation conducting the surveillance takes counter measures. The important point, however, is that these activities, though sometimes decried, have always been practiced, and are consistent with norms of territorial sovereignty and the limitations on enforcement jurisdiction.[51]

III. THE VALIDITY AND LIMITS OF REMOTE CROSS-BORDER SEARCHES

With these examples and principles in mind, we return to remote cross-border searches on the internet. Many analogize these cross-border searches to physical invasion of police forces into another territory. But the analogy is not persuasive. Such searches are, instead, better analogized to the grand jury orders and spy techniques outlined above. Cross-border searches and seizures are like grand jury orders because they leverage power in the United States to achieve disclosure of information abroad. And they are like spy techniques because they use a universal medium to observe events in another country. Seen this way, remote cross-border searches fit into the long-accepted practice of officials in one nation acting within their territory (or from public spaces) to extract information from another.

These analogies are not perfect, of course. The costs of cross-border internet searches are lower than many other exercises of extraterritorial influence. As a result, one might worry that the potential for abuse in the use of internet cross-border searches and seizures is higher than more traditional counterparts, like grand jury orders. The point so far has been simply to show that international law principles of enforcement jurisdiction do not clearly prohibit such searches, and that the concept of "territorial sovereignty" by itself does little, if any, analytical work in determining the validity of such searches under international law. There is little doubt that if such searches prove necessary to redress cross-border internet attacks, international law will adapt to permit them in some circumstances. As we have seen, the his-

---

[51] Under international law, nations enjoy exclusive authority over the airspace above their territory, but this authority does not extend to outer space. Therefore, one nation's satellite may orbit over the territory of another and gather information without permission. See Joseph A. Bosco, *International Outer Space Law: A Brief Overview*, 9 Air & Space Law 3, 5 (Spring 1995). Such satellite surveillance is justified by analogy to surveillance from the high seas, which has long been viewed as legal. Robert A. Ramey, *Armed Conflict on the Final Frontier: The Law of War in Space*, 48 AF L Rev 1, 65 (2000); John Kish, *International Law and Espionage* 115–120 (Kluwer 1995) (David Turns, ed).

tory of international jurisdiction is one of the law accommodating the nations' felt needs to take steps within their borders to redress local harms caused from abroad that cannot otherwise be addressed. Nations will not, and cannot, be expected to acquiesce in the face of a damaging cross-border attack. As the *Trail Smelter* arbitration panel said in a different but related context, "no state has the right to use or permit the use of its territory in such a manner as to cause injury . . . in or to the territory of another."[52]

There are essentially two responses to these arguments. One is a worry that remote cross-border searches will be abused—that nations will conduct such searches when other, less offensive means might achieve the same end. The second response is based on a worry about reciprocity and retaliation. If FBI officials can engage in remote cross-border searches, then governmental officials—not to mention private parties—in other countries can do the same to U.S. computer databases. The practice threatens to spin out of control, resulting in massive violations of territorial sovereignty and computer privacy that make all nations worse off.

These are understandable concerns. But I believe that they will prove to be unfounded. Just as there is every reason to think that remote cross-border searches will be necessary in some circumstances, there is every reason to believe that sensible limits on cross-border searches will develop. They will develop not as a deduction from legal concepts like territorial sovereignty. Instead, they will emerge the way all new principles of customary international law emerge: through a process of trial and error, thrust and counterthrust, as nations accommodate themselves to the costs and benefits of a new technology and its regulation.

As an initial matter, the two concerns expressed above—abuse and reciprocity—will cancel one another out to some extent. Nations tend to be aggressively extraterritorial when they can get away with it, but they tend to check extraterritorial action when it can be reciprocated to their detriment. In this sense, the ease with which the internet permits cross-border searches will operate as a natural check on aggressive cross-border searches. In the internet context, the United States cannot, as it has in "real space" for decades, engage in aggressive extraterritorial activity with impunity. The consternation in the United

---

[52] *United States v Canada*, 3 R Intl Arb Awards 1905, 1965 (1938).

States over the European Data Protection Initiative,[53] and the recent French court injunction on the U.S. firm Yahoo!'s web auctions,[54] shows that the internet is potentially a great equalizer of extraterritorial authority.

Because aggressive cross-border searches can easily be reciprocated, governments will have incentives to limit their searches to exigent circumstances, and to work out cooperative principles where possible. Another important reason to expect limits on cross-border searches is that a search, by itself, is usually not very helpful in bringing a cybercriminal to justice in the target state. In most circumstances, the target nation will need the cooperation—through extradition or some similar arrangement—of the source country to actually enforce U.S. law against criminal defendants.[55] Cross-border searches viewed as illegitimate by a source country will not incline that country to provide such cooperation.

Finally, nations that are subject to cross-border searches will have incentives to provide meaningful and hurried assistance in redressing crimes that originate from their borders. For to the extent they provide such assistance, there will be less need for unilateral cross-border searches. This in a nutshell is why there has been such enthusiastic agreement among participating nations on the cooperative aspects of the European Cybercrime Convention.

CONCLUSION

This essay has argued that cross-border searches are a necessary tool in the fight against cross-border cybercrime. It has tried to show that such searches are not prohibited by norms of territorial sovereignty, and are not without precedent. It has also tried to sketch the norms that are likely to emerge in the exercise

---

[53] On the debate sparked by the European Data Protection Initiative, see generally Peter P. Swire and Robert Litan, *None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive* (Brookings 1998).

[54] See Jack L. Goldsmith, *Yahoo! Brought Down to Earth*, Fin Times, Comment & Analysis 27 (Nov 26, 2000).

[55] The opening example of the Russian hackers is a counterexample. There, U.S. officials were able to lure the Russian criminals into the United States, where they were apprehended and charged. See Lemos, *Lawyers Slam FBI 'Hack,'* ZDNet News (cited in note 1); Linn, *FBI's Elaborate Hacker Sting*, Chi Trib at 20 (cited in note 1). One of the Russian hackers was found guilty of multiple counts of fraud, conspiracy, and computer crimes while the other awaited trial in New Jersey. See Michelle Delio, *'Stung' Russian Hacker Guilty*, Wired News (Oct 17, 2001); available online at <http://www.wired.com/news/print/0,1294,47650,00.html> (visited Oct 20, 2001) [on file with U Chi Legal F].

of such searches, as well as the reasons why these norms will emerge.

In light of these arguments, the early uses of unilateral extraterritorial enforcement measures should not be viewed as an illegitimate invasion of another nation's sovereignty. Cross-border searches and seizures should be viewed instead as part of the inevitably messy process of working out new customary principles of sovereignty to accommodate a new and important, but also potentially dangerous, technology.