

# New Objectives for CFIUS: Foreign Ownership, Critical Infrastructure, and Communications Interception

**James A. Lewis\***

I. NEW CHALLENGES.....	458
II. THE CFIUS PROCESS .....	463
III. RISKS OF FOREIGN OWNERSHIP.....	472
IV. NEW GOALS FOR REGULATION.....	476

Global economic integration creates new kinds of risks for national security. Foreign ownership of U.S. telecommunications service providers is one such risk. While foreign acquisitions of U.S. companies are almost always harmless, there has always been concern among federal officials that foreign ownership could multiply opportunities for espionage, make defenders' tasks more complex, and reduce law enforcement communications interception capabilities. A new concern is that foreign acquisitions are a new avenue for a potential opponent to disrupt critical infrastructure and the services. The issue for national security is how to preserve communications interception capabilities and defend against potential service disruptions or intelligence activities in a period where

---

\* James Andrew Lewis is a Senior Fellow and Director of the Technology and Public Policy program at the Center for Strategic and International Studies, a research center in Washington, D.C. Before coming to CSIS, Lewis was a career diplomat who worked on a range of national security and technology-related issues at the Departments of State and Commerce, the National Security Council, and with U.S. military commands.

integrated, global telecommunications enterprises and foreign ownership of, or participation in, national networks is increasingly routine.

### I. NEW CHALLENGES

Communications interception is an integral part of law enforcement and intelligence activities. Nations have engaged in the interception of electronic communications for more than a century. Most countries have agencies, policies, and legal structures that control and take advantage of interception techniques. These control mechanisms also secure the country's own communications networks and information from the interception efforts of others.<sup>1</sup>

Communications interception techniques can be divided into two broad categories: bulk interception and targeted interception. Bulk interception is the collection of all signals or emanations regardless of who sends them. The mass of signals are then processed and filtered to discover meaningful information. This technique is primarily used by intelligence agencies and is derived from military signals intelligence efforts that began shortly before World War I when militaries began to monitor the radio spectrum for transmissions of interest.<sup>2</sup> The zenith for bulk collection efforts was in the 1980s and since then the effectiveness of these techniques has been degraded by advances in information technology.<sup>3</sup>

The second category, targeted interception, involves collecting against an individual user or device. This includes the techniques that fall under the rubric of wiretapping, but also new techniques developed for targeted collection on the Internet (these techniques often resemble spyware). Targeted collection frequently requires intrusive measures (as opposed to the more passive bulk collection techniques) which involve direct physical access to the communications medium or to the physical space of the target to collect data. It is difficult and costly to do this covertly. Targeted collections, and their requirement for access, are more intrusive and can pose a greater risk to civil liberties.

The Committee on Foreign Investment in the United States ("CFIUS") is part of a broader effort in the United States to maintain interception capabilities. The United States seeks to preserve its

---

1. Eur. Parl. Doc., Report on the Existence of a Global System for the Interception of Private and Commercial Communications (A5-0264/2001) 27–28 (2001), available at [http://www.fas.org/irp/program/process/rapport\\_echelon\\_en.pdf](http://www.fas.org/irp/program/process/rapport_echelon_en.pdf) [hereinafter Interception of Communications].

2. See generally John Keegan, *Intelligence in War: Knowledge of the Enemy From Napoleon to Al-Qaeda* (2003).

3. See *id.* at 14–16. See also JAMES BAMFORD, *BODY OF SECRETS: ANATOMY OF THE ULTRA-SECRET NATIONAL SECURITY AGENCY* 647–48 (First Anchor Books 2002) (2001).

interception capabilities while limiting foreign interception opportunities. Since the end of the Cold War, implementation of this policy has required repeated responses to changes in technology that would have otherwise degraded U.S. capabilities. The technological improvements that made communications technologies better and cheaper can also make interception more difficult. These improvements included the use of fiber optics, packet switching, strong commercial encryption, and the spread of Voice over Internet Protocol (“VoIP”).<sup>4</sup> Many of the regulatory battles between the federal government and the telecommunications and information technology industry in the 1990s, such as the Communications Assistance to Law Enforcement Act (“CALEA”), encryption, Carnivore, Patriot Act modifications to the Foreign Intelligence Surveillance Act (“FISA”)—involved federal efforts to constrain or respond to technological change.

Technological challenges to interception are now complemented by challenges that arise from changes in the international economic environment: the globalization of supply chains and ownership, especially foreign ownership of U.S. telecommunications networks. This new challenge will shape future policy and regulatory interventions of communications interception.

This development has grown out of a broader set of economic and political changes. These changes have made the task of interception more difficult. Regulations that emphasize private ownership and competition in telecommunications have reduced the number of national monopoly service providers that, since they were very often owned completely or in part by the government or were themselves a government agency, had a tradition of close cooperation with national authorities. Regulatory changes and improved technologies have lowered the cost of communications and helped contribute to growth in the volume of traffic, which also complicates intelligence activities.<sup>5</sup> The profusion of services, technologies, and service providers also complicates interception efforts. The economic benefit of these changes clearly outweighs the cost to law enforcement and intelligence, but few governments appear to be willing to accept the accompanying erosion of capabilities.

A more gradual set of challenges to interception emerged from the regulatory and policy changes that encouraged global economic integration

---

4. “[M]odern telecommunications technology poses significant challenges to [signals intelligence]. . . .” National Security Agency/Central Security Service, Signals Intelligence, at <http://www.nsa.gov/sigint/index.cfm> [hereinafter Signals Intelligence]. See also BAMFORD, *supra* note 3, at 440–63.

5. See Signals Intelligence, *supra* note 4; BAMFORD, *supra* note 3, at 440–63; Interception of Communications, *supra* note 1, at 27–28.

and the internationalization of ownership. American foreign policy for more than a century has encouraged an open, international economy and the removal of restrictions to trade and foreign investment. Technological change reinforces globalization. Expanded trade, new technologies, and the resultant international economic integration changed how companies must do business if they want to remain financially and technologically viable. These changes, however, have created a new series of concerns in the national security community.

The crux of these concerns is that the United States faces new kinds of threats to its defense that fall outside of traditional military and intelligence activities. This belief grows out of changes in the international security and economic environment that followed the end of the Cold War. A series of commissions grappled with the problem of how to adjust U.S. security policies in the new environment in the 1990s. These commissions concluded that national security would face new kinds of threats from opponents, who would use unconventional and asymmetrical modes of attack with unconventional weapons, and exploit vulnerabilities within the American infrastructure.<sup>6</sup> Weapons of mass destruction formed the principle source of asymmetrical threats to the homeland, but information and communications systems were also seen as especially vulnerable.<sup>7</sup> This highlights the emphasis in homeland security on new threats to security and a new sense of vulnerability that pervades policymaking.<sup>8</sup>

There is no coherent strategy in the United States for dealing with these issues, in part because they are new and in part because they cut across the responsibilities of existing agencies. Much of the activity in national security during the last ten years, beginning with Presidential

---

6. Frank Cilluffo et al., Center for Strategic and International Studies, *Defending America in the 21st Century: New Challenges, New Organizations, and New Policies* (2000) (providing an executive summary of four CSIS working group reports on homeland defense), available at <http://www.csis.org/burke/hd/reports/defendamer21stexecsumm.pdf>.

7. "Our economy and national security are fully dependent upon information technology and the information infrastructure." White House, *The National Strategy to Secure Cyberspace* viii (Feb. 2003), available at [http://www.whitehouse.gov/pcipb/cyberspace\\_strategy.pdf](http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf) [hereinafter *Secure Cyberspace*].

8. The reports include: The Joint Security Commission, *Redefining Security: A Report to the Secretary of Defense and the Director of Central Intelligence* (1994), at <http://www.loyola.edu/dept/politics/intel/jsc-report.pdf>; Defense Science Board, Dept. of Defense, *Report of the Defense Science Board Task Force on Information Warfare—Defense* (1996), at <http://www.acq.osd.mil/dsb/reports/iwd.pdf>; National Commission on Terrorism, *Countering the Changing Threat of International Terrorism* (2000), at <http://www.loyola.edu/dept/politics/intel/terrorism/NCTReport2000.pdf>; National Defense Panel, *Transforming Defense: National Security in the 21st Century* (1997), at <http://www.dtic.mil/ndp/FullDoc2.pdf>; The President's Commission on Critical Infrastructure Protection, *Critical Foundations: Protecting America's Infrastructures* (1997), at <http://www.tsa.gov/interweb/assetlibrary/Infrastructure.pdf>.

Decision Directive 63 on Critical Infrastructure Protection,<sup>9</sup> the creation of the Department of Homeland Security, and the publication of both the National Strategy for the Physical Protection of Critical Infrastructures and Key Assets<sup>10</sup> and the National Strategy to Secure Cyberspace,<sup>11</sup> focused on developing a policy framework for a new security environment where a territorial concept of security is no longer adequate to describe the nature or source of potential threats.<sup>12</sup>

In the earlier territorial concept of security, borders were clearly demarcated, industries were national, and key services were state-owned or provided by national firms. This made the management of security tasks (such as communications interception) easier for national authorities. However, the economic underpinnings of this territorial approach have been eroded. Agreements on international trade and finance, buttressed by technological developments, made it easier for nationals of one country to own and invest in companies and provide services in another country.<sup>13</sup> International agreements to remove regulatory obstacles for foreign ownership, combined with national economic policies that privatize and deregulate key services are increasing the integration of national economies.

Opening the door for American companies to sell or own property outside the United States has been a hallmark of American foreign policy. The United States routinely seeks bilateral and multilateral investment trade agreements to promote free trade. The recent focus of trade liberalization was to remove barriers to direct foreign investment and ownership by foreign nationals of key services, such as telecommunications.<sup>14</sup> The 1998 World Trade Organization Basic

---

9. White House, Presidential Decision Directive/NSC-63: Critical Infrastructure Protection (May 1998), available at <http://www.fas.org/irp/offdocs/pdd/pdd-63.htm>.

10. See WHITE HOUSE, THE NATIONAL STRATEGY FOR THE PHYSICAL PROTECTION OF CRITICAL INFRASTRUCTURES AND KEY ASSETS (Feb. 2003), available at [http://www.whitehouse.gov/pcipb/physical\\_strategy.pdf](http://www.whitehouse.gov/pcipb/physical_strategy.pdf) [hereinafter INFRASTRUCTURE PROTECTION].

11. See SECURE CYBERSPACE, *supra* note 8.

12. "In the last century, geographic isolation helped protect the United States from direct physical invasion. In cyberspace national boundaries have little meaning." *Id.* at 7. See also INFRASTRUCTURE PROTECTION, *supra* note 11.

13. Trade in Telecommunications Services: Before the House Commerce Subcomm. on Telecomm., Trade and Consumer Protection, Comm. on Commerce, 106th Cong. (2000), available at [http://www.usembassy.it/file2000\\_09/alia/a0090716.htm](http://www.usembassy.it/file2000_09/alia/a0090716.htm) (testimony of Richard W. Fisher, Deputy U.S. Trade Rep.) [hereinafter Fisher Testimony on Telecommunications Services].

14. See, e.g., Director General, Supachai Panitchpakdi, Introductory Remarks at the WTO Public Symposium: WTO After Ten Years: Global Problems and Multilateral Solutions (Apr. 20, 2005), at [http://www.wto.org/english/news\\_e/spsp\\_e/spsp38\\_e.htm](http://www.wto.org/english/news_e/spsp_e/spsp38_e.htm).

Agreement on Telecommunications Services expanded the ability of foreign owners (with certain caveats detailed in the agreement)<sup>15</sup> to enter telecommunications markets and furthered the trends in technology, causing partnering agreements and ownership in telecommunications to be increasingly linked across borders.<sup>16</sup> Negotiations in the World Trade Organization (“WTO”) furthered liberalizations in the trade of telecommunications services.<sup>17</sup>

The results of consolidation in the telecommunications industry, and the effect of WTO agreements that break down the barriers to firms in one country providing services in another, have increased the blending of ownership. However, while American firms were investing overseas, foreign firms were investing in the United States. Foreign investment is vital to the national economy and the United States could not deny to others the rights it has sought for itself. Some forms of investment, where a foreign entity assumes ownership and control of a U.S. plant or facility, raise national security concerns. Telecommunications services are now routinely provided through cross-border arrangements between companies. Increasingly, services are also provided by foreign-owned firms that own and operate telecommunications networks.

Communications interception poses an indirect, but real challenge for critical infrastructure. In part, this is because the United States defined critical infrastructure protection to include information assurance. Communications interception is problematic because of concerns that access to information networks could provide the capability to disrupt critical services. Communications interception capabilities are, in essence,

---

15. WORLD TRADE ORGANIZATION, FOURTH PROTOCOL TO THE GENERAL AGREEMENT ON TRADE IN SERVICES (April 30, 1996), at [http://www.wto.org/english/docs\\_e/legal\\_e/4prote\\_sl20\\_e.pdf](http://www.wto.org/english/docs_e/legal_e/4prote_sl20_e.pdf). The Fourth Protocol, which applied to basic telecommunications services, entered into force on January 1, 1998.

16. See FEDERAL COMMUNICATIONS COMMISSION, INTERNATIONAL BUREAU, REPORT ON INTERNATIONAL TELECOMMUNICATIONS MARKETS 2000 UPDATE 3–4 (May 2001); World Trade Organization, Fourth Protocol to the General Agreement on Trades in Services, April 30, 1996, S/L/20 (96-1750), available at [http://www.wto.org/english/docs\\_e/legal\\_e/4prote\\_sl20\\_e.pdf](http://www.wto.org/english/docs_e/legal_e/4prote_sl20_e.pdf); INTERNATIONAL TELECOMMUNICATIONS UNION, GLOBAL MARKET TRENDS, ITU NEWS (2003).

The United States, through the FCC, responded to the 1996 agreement in the WTO, by issuing two implementing orders to allow foreign investors from WTO member states to enter the market: the *Foreign Participation Order*, and the *DISCO II Order*. Both orders appeared in 1997. See Rules and Policies on Foreign Participation in the U.S. Telecomm. Mkt., *Report and Order*, 12 F.C.C.R. 23,891 (1997); Amendment of the Commission’s Regulatory Policies to Allow Non-U.S. Licensed Space Station to Provide Domestic and Int’l Satellite Serv. in the United States, *Report and Order*, 12 F.C.C.R. 24,094 (1997).

17. WORLD TRADE ORGANIZATION, *Telecommunications Services*, at [http://www.wto.org/english/tratop\\_e/serv\\_e/telecom\\_e/telecom\\_e.htm](http://www.wto.org/english/tratop_e/serv_e/telecom_e/telecom_e.htm) (last visited Apr. 11, 2005).

a critical government service provided by telecommunications companies. The National Strategy to Secure Cyberspace was formulated, in part, to describe initiatives to “secure our information systems against deliberate, malicious disruption”<sup>18</sup> and to identify “strategic information warfare” as a source of catastrophic risk for the Homeland Security Strategy.<sup>19</sup>

## II. THE CFIUS PROCESS

The United States has three regulatory vehicles to control foreign ownership in the telecommunications sector. These vehicles are vested in the Department of the Treasury, the Federal Communications Division, and—to a lesser extent—the Department of Justice (“DOJ”).<sup>20</sup> The first of these vehicles is the Federal Communications Commission’s (“FCC”) ability to review the transfer of licenses.<sup>21</sup> The Communications Act of 1934 prohibits the transfer of an FCC license to a corporation of which a foreign government owns 25 percent or more, but gives the FCC the authority to waive this provision if it judges the license to be in the public interest.<sup>22</sup> The FCC routinely defers, however, to executive branch agencies, such as the DOJ and the Department of Defense in determining the effect of the acquisition on national security. The second of these vehicles is the DOJ’s ability to review the proposed purchase for antitrust implications.<sup>23</sup> The third and most important of these three vehicles is the Treasury Department’s chaired CFIUS. The United States created the CFIUS process in 1988 as part of a larger trade liberalization policy to review the potential national security implications of foreign acquisitions of U.S. firms. Section 5021 of the landmark Omnibus Trade and Competitiveness Act of 1988 amended section 721 of the Defense Production Act of 1950 to give the President the authority to suspend or prohibit any foreign acquisition, merger, or takeover of a U.S. corporation that is determined to threaten national security.<sup>24</sup>

---

18. OFFICE OF HOMELAND SECURITY, NATIONAL STRATEGY FOR HOMELAND SECURITY 5 (2002), available at [http://www.whitehouse.gov/homeland/book/nat\\_strat\\_hls.pdf](http://www.whitehouse.gov/homeland/book/nat_strat_hls.pdf).

19. *Id.* at 2.

20. *Fisher Testimony on Telecommunications Services*, *supra* note 14 (identifying the “tools available to address competition and national security concerns posed by foreign government ownership” as the FCC’s Public Interest Test (particularly section 310(b)(4) of the Communications Act of 1934)).

21. Communications Act of 1934, § 310, 48 Stat. 1064 (codified at 47 U.S.C. § 310).

22. § 310(a), (b)(4).

23. See DEPARTMENT OF JUSTICE, ANTITRUST DIVISION MANUAL, CH. II: STATUTORY PROVISIONS AND GUIDELINES OF THE ANTITRUST DIVISION, at <http://www.usdoj.gov/atr/foia/divisionmanual/ch2.htm> (last visited April 3, 2005).

24. See EUROPEAN COMMISSION, REPORT ON UNITED STATES BARRIERS TO TRADE AND INVESTMENT 59 (Brussels, Dec. 2003), available at <http://trade-info.cec.eu.int/doclib/>

CFIUS is an interagency body staffed by midlevel officials and chaired by the Treasury Department. The Departments of Defense, State, Justice, and Commerce are among the agencies that participate in the CFIUS process. Representatives from the Federal Bureau of Investigation ("FBI") and the intelligence community are also involved, sometimes in an advisory capacity. President Bush made the Department of Homeland Security ("DHS") a member of CFIUS in February 2003.<sup>25</sup> CFIUS was originally created to monitor the economic implications of foreign investment in the United States, which is why the Treasury Department chairs it; but in 1988, Congress gave it the role of reviewing the national security implications of foreign acquisitions of U.S. companies. This is now its most important function.<sup>26</sup>

Most foreign purchasers are not required to file with CFIUS, but if they do not and CFIUS later decides that it objects to the purchase, the United States can force the new foreign owner to divest itself of the acquisition. Many companies decide it is safer to notify the Treasury Department. After notification, CFIUS has one month in which to decide whether or not to investigate the proposed sale. If it does not choose to investigate, the sale can proceed. CFIUS finds very few submissions warrant investigation. Only a few of the more than two thousand notifications received by CFIUS since 1988 were investigated, and of these, only one was blocked.<sup>27</sup> In most cases, if CFIUS chooses to open an

---

docs/2003/december/tradoc\_115383.pdf.

25. Press Release, The White House, Office of the Press Secretary, Executive Order Amendment of Executive Orders, and Other Actions, in Connection with the Transfer of Certain Functions to the Secretary of Homeland Security (Feb. 28, 2003), at <http://www.whitehouse.gov/news/releases/2003/02/print/20030228-8.html> [hereinafter Homeland Security Executive Order].

26. OFFICE OF INTERNATIONAL INVESTMENT, DEPARTMENT OF TREASURY, COMMITTEE ON FOREIGN INVESTMENT IN THE UNITED STATES, *Exon-Florio Provision*, at <http://www.treas.gov/offices/international-affairs/exon-florio/> (last visited Apr. 3, 2005) [hereinafter *Exon-Florio Provision*].

27. In 1990, a Chinese firm was ordered to divest itself of an U.S. aircraft parts manufacturer. Details are as follows:

[I]n February 1990 . . . President Bush ordered CATIC, the import-export arm of the Ministry of Aerospace Industry of the People's Republic of China, to divest its interest in MAMCO, a privately owned, Seattle-based manufacturer of civilian airplane parts, primarily for Boeing. Although CATIC notified CFIUS of the proposed acquisition, the transaction was closed before completion of the initial review period. The sale was perfectly legal, but it turned out to be an unfortunate and costly decision when President Bush later ordered divestiture.

Susan W. Liebeler and William H. Lash III, *Exon-Florio: Harbinger of Economic Nationalism?*, REGULATION, Winter 1996, available at <http://www.cato.org/pubs/regulation/reg16n1d.html>.

A variety of sources carry statistics on CFIUS cases. See General Accounting Office, *Implementation of Exxon Florio and related Amendments*, at 3-4 (Dec. 1995), at



investigation, companies respond by abandoning the planned acquisition or, in a smaller number of cases, by offering to restructure the acquisition in a way that addresses the security concerns raised by CFIUS. In 2004, CFIUS reviewed forty-five cases and referred only one to the President for a decision.<sup>28</sup>

The formal CFIUS review is not the most important element in the approval process. CFIUS does not require unanimity among all the agencies involved, but a disputed decision to approve a sale would be escalated to the cabinet level or to the President for appeal.<sup>29</sup> The Treasury Department has been reluctant to engage in such escalation. The timelines for decision included in the authorizing legislation to ensure a speedy CFIUS decision can be suspended by the Treasury Department in a process known as “stopping the clock,” usually justified on the grounds that further information is needed from the purchaser. Most applicants support this delay since the alternative is potential rejection.<sup>30</sup> In effect, this gives individual agencies a kind of de facto veto that allows them to use the pending CFIUS decision to gain leverage and concessions from foreign purchasers.

Until now, the most influential agencies in the CFIUS process were the Department of Defense and the DOJ. These are also the agencies most likely to be affected by a foreign purchase. Both agencies will often defer casting their vote in CFIUS until such time as they have been able to arrange side agreements with the foreign purchaser that assuage their security concerns.<sup>31</sup>

The Department of Defense’s concerns in cases involving telecommunications focus on communications security.<sup>32</sup> The Department

---

<http://www.fas.org/asmp/resources/govern/gao9612.pdf>; Deputy Under Secretary of Defense for Industrial Policy, Frequently Asked Questions: What is CFIUS?, at <http://www.acq.osd.mil/ip/faq.html#number5> (last visited May 2, 2005); Department of the Treasury, Annual Performance Report: Performance and Accountability Report FY 2004, pt. II, at 47 (2004), at <http://www.treas.gov/offices/management/dcfo/accountability-reports/2004reports/part2.pdf> (last visited May 2, 2005); Akin Gump Strauss Hauer & Feld LLP, International Trade Alert: CFIUS National Security Review Creates New Uncertainty for Foreign Investment in the United States, (May 2003), at <http://www.akingump.com/docs/publication/562.pdf> [hereinafter Akin Trade Alert].

28. Department of the Treasury, Annual Performance Report: Performance and Accountability Report FY 2004, pt. II, at 47 (2004), at <http://www.treas.gov/offices/management/dcfo/accountability-reports/2004reports/part2.pdf> (last visited May 2, 2005).

29. See 31 C.F.R. pt. 800, subpts. E, F (2003).

30. See 31 CFR § 800.403 (2003).

31. See Bryan Tramont, *Too Much Power, Too Little Restraint: How the FCC Expands its Reach Through Unenforceable and Unwieldy ‘Voluntary’ Agreements*, 53 FED. COMM. L.J. 49, 53–54 (2000).

32. The Department of Defense’s primary concern in most CFIUS cases is to prevent

of Defense built on the CFIUS process by suggesting that defense-related firms meet informally with Department of Defense staff before making a submission to CFIUS.<sup>33</sup> Companies that do not informally consult with the Department of Defense run the risk of having the Department of Defense announce that the thirty days allowed by law were not enough to review the transaction.<sup>34</sup> Some firms have had to temporarily withdraw their CFIUS petitions in order to give the Department of Defense more time. Withdrawal is often done to propose and work out arrangements with the acquiring party that place restrictions on the acquisition to resolve national security concerns.<sup>35</sup> The Department of Defense's own regulations, such as the National Industrial Security Program Operating Manual reinforce CFIUS by requiring notification and approval of foreign acquisitions or mergers from companies that operate cleared facilities.<sup>36</sup>

The goals of the DOJ and the FBI in CFIUS cases involving telecommunications or network services include both communications security and ensuring a continued ability to engage in communications interception. Avoiding degradation to communications interception usually formalizes understandings with the new owner that U.S. law regarding communications interception, as opposed to the laws of the purchasing country, continues to apply and that the informal cooperation often obtained from U.S. service providers will continue with the new foreign-owned entity. In some cases, assurances are sought that network operations data, which is of use to law enforcement, will continue to be stored in the United States or that the corporation will create special U.S. citizen-only units to handle law enforcement requests.<sup>37</sup>

---

the illicit acquisition or transfer of technology by the new foreign owners. See OFFICE OF THE UNDER SECRETARY OF DEFENSE FOR ACQUISITIONS, TECHNOLOGY AND LOGISTICS, DEPARTMENT OF DEFENSE, INDUSTRIAL POLICY: FREQUENTLY ASKED QUESTIONS, at <http://www.acq.osd.mil/ip/faq.html> (last visited April 3, 2005).

33. Deputy Under Secretary of Defense for Industrial Policy, Frequently Asked Questions: What is CFIUS?, at <http://www.acq.osd.mil/ip/faq.html#number5> (last visited May 2, 2005). The site specifically states:

Firms that are planning a CFIUS filing that involves sensitive and/or extensive defense contracts are encouraged to meet informally with staff of DUSD (Industrial Policy) and other relevant DoD components prior to formal CFIUS notification so that DoD analysis of the transaction can begin before the start of the 30-day initial review clock.

34. *Id.*

35. See *id.*; John B. Reynolds, III, Foreign Direct Investment in U.S. Critical Infrastructure (2004), at [http://www.wrf.com/publication.cfm?pf=1&publication\\_id=11735](http://www.wrf.com/publication.cfm?pf=1&publication_id=11735).

36. DEPARTMENT OF DEFENSE, NATIONAL INDUSTRIAL SECURITY PROGRAM OPERATING MANUAL, Ch. II, Sec. 3 (1995, incorporating changes through 2001), available at <http://www.dss.mil/isec/nispom.pdf> [hereinafter DEPARTMENT OF DEFENSE OPERATING MANUAL].

37. Reynolds, *supra* note 36.

One indication of the changing policy interests that drives CFIUS and foreign ownership concerns is the addition of the DHS via presidential directive.<sup>38</sup> The DHS's role and influence in CFIUS reviews of foreign telecommunications acquisitions was strengthened by the transfer of the National Communications System ("NCS")—an agency created in the Kennedy Administration to improve, secure, and increase the survivability of the telecommunications network.<sup>39</sup> Originally part of the Department of Defense, the NCS is now part of the DHS's infrastructure protection directorate and provides the agency with expertise and long-standing relationships with service providers.<sup>40</sup>

The concerns raised by the FBI, the DOJ, or the Department of Defense are usually resolved through the negotiation of a Network Security Agreement, a document, usually confidential, that lays out conditions to which a foreign purchaser must adhere for the transaction to win CFIUS approval.<sup>41</sup> These conditions can include limiting the performance of certain functions to U.S. citizens; establishing understandings on where data will be stored, often a requirement that data remain in the United States; or, in more draconian agreements, restructuring the new, foreign-owned corporation to create "firewalls" between the new owners and security-related functions.<sup>42</sup>

The DOJ or the Department of Defense, and now the DHS, negotiate Network Security Agreements directly with the foreign purchaser, without the full participation of CFIUS members and independent of the CFIUS review.<sup>43</sup> The chief weakness in Network Security Agreements lies not in their negotiation, but in what follows, or rather, what does not follow—the inability or lack of ensuring compliance.

Once a Network Security Agreement is reached and CFIUS approval granted, there is no systematic process in CFIUS to assign an agency the

---

38. Homeland Security Executive Order, *supra* note 26.

39. NATIONAL COMMUNICATIONS SYSTEM, BACKGROUND AND HISTORY OF THE NCS, *at* <http://www.ncs.gov/about.html> (last reviewed Mar. 22, 2004).

40. *See* 31 C.F.R. pt. 800, subpts. E, F (2003).

41. While most network security agreements are not public, their existence is not secret. *See* Reynolds, *supra* note 36; Steptoe and Johnson, Law Enforcement and Technology Practice, *at* [http://www.steptoelaw.com/index.cfm?fuseaction=ws.DspSite&site\\_id=462](http://www.steptoelaw.com/index.cfm?fuseaction=ws.DspSite&site_id=462) (last visited May 2, 2005); Akin Trade Alert, *supra* note 28.

42. *See, e.g.*, GLOBAL CROSSING CORPORATION, RAISING THE BAR FOR NETWORK SECURITY: THE NETWORK SECURITY AGREEMENT AMONG GLOBAL CROSSING, ST TELEMEDIA AND SEVERAL U.S. GOVERNMENT AGENCIES, *available at* [http://www.globalcrossing.com/xml/network/net\\_security.xml](http://www.globalcrossing.com/xml/network/net_security.xml). (last visited Apr. 3, 2005) (discussing the specific terms that Global Crossing agreed to in its Network Security Agreement).

43. *See, e.g.*, Global Crossing Ltd. et al., Applications for Consent to Transfer Control of Submarine Cable Landing Licenses, *Order and Authorization*, 18 F.C.C.R. 20,301, Sec. F (2003).

responsibility for ensuring compliance and there is no systematic effort to enforce Network Security Agreements. A similar weakness is the lack of clarity as to which agency has authority to enforce the agreements. The lack of enforcement to ensure compliance with a Network Security Agreement makes the entire process somewhat questionable. There is some speculation that either the DHS will claim that it has this responsibility or that the White House will assign the DHS this responsibility via a new presidential directive as part of its larger infrastructure protection responsibilities.

In recent years, the most challenging cases before CFIUS involved the telecommunications and information technology sectors, as European and Asian firms sought to acquire telecommunications service providers like VoiceStream, Global Crossing, or high-tech manufacturers like Silicon Valley Group ("SVG").<sup>44</sup> Three trends—privatization, the introduction of new services, and successful efforts in the WTO to break down the barriers to firms in one country providing telecommunications services in other countries—created international opportunities that attract foreign ownership.

The most salient case involves Global Crossing. Its \$20 billion global fiber optic network crosses both the Atlantic and Pacific oceans and connects twenty-seven countries in Asia, North and South America, and Europe. Global Crossing provided key services to a broad range of U.S. entities in both the public and private sectors, including the Department of Defense.<sup>45</sup> The company filed for bankruptcy in 2002 and was the target of several acquisition attempts, including offers by foreign companies.<sup>46</sup> The bid by Hong Kong firm Hutchison Whampoa raised serious national

---

44. SVG is a United States manufacturer of leading edge photolithography technologies that was bought by a Netherlands company. JOSEPH LIEBERMAN, SENATE ARMED SERVICES COMMITTEE, WHITE PAPER: NATIONAL SECURITY ASPECTS OF THE GLOBAL MIGRATION OF THE U.S. SEMICONDUCTOR INDUSTRY 9 (2003), available at [http://www.fas.org/irp/congress/2003\\_cr/s060503.html](http://www.fas.org/irp/congress/2003_cr/s060503.html); Press Release, Senate Republican High Tech Task Force, High Tech Task Force Members Urge Expeditious Review of SVG-ASML Merger (Apr. 11, 2001), at [http://republican.senate.gov/httf/index.cfm?FuseAction=PressReleases.Detail&PressRelease\\_id=10&Month=4&Year=2001](http://republican.senate.gov/httf/index.cfm?FuseAction=PressReleases.Detail&PressRelease_id=10&Month=4&Year=2001). See also Jeff Chappel, *Politics Hamper SVG-ASML Merger*, ELECTRONIC NEWS, Mar. 12, 2001, at <http://www.reed-electronics.com/electronicnews/article/CA66153.html>; David Richardson, Foreign Investment and the Australia United States Free Trade Agreement, Parliament of Australia, Economics, Commerce and Industrial Relations Group, Current Issues Brief No. 7 2003-04, (Mar. 2004), available at <http://www.aph.gov.au/library/pubs/CIB/2003-04/04cib07.pdf>.

45. See, e.g., Press Release, Global Crossing, Global Crossing Wins Network Services Contract From U.S. Department of Defense Valued up to \$400 Million (July 9, 2001), available at <http://www.globalcrossing.com/xml/news/2001/july/09.xml>.

46. Reuters, *Global Crossing Says Has More than 60 Suitors* (May 8, 2002), available at <http://www.usatoday.com/money/telecom/2002-05-08-global-suitors.htm>.

security concerns within the U.S. government. After a protracted CFIUS review in the face of considerable hostility toward Hutchison from some agencies, Hutchison Whampoa's offer was withdrawn.<sup>47</sup>

Singapore Technologies Telemedia ("STT") ultimately purchased Global Crossing in December 2003 (after CFIUS approval in September and FCC approval in October).<sup>48</sup> STT holds a 71 percent share of the company. Despite the conclusion of a free trade agreement between Singapore and the United States, STT also faced some opposition, in part because STT is partially owned by the Singaporean government.<sup>49</sup>

The crux of the opposition to Hutchison was the company's alleged connections to the Chinese government.<sup>50</sup> Senior Chinese government officials are reputedly among Hutchison's stockholders. The Department of Defense and others feared that China could use this investment relationship to influence Hutchison and particularly to obtain access to Global Crossing's communications networks; Hutchison's bid was hurt by these allegations. Hutchison is clearly a legitimate, commercial, publicly-traded entity with a long history of business success, but Chinese intelligence entities have used their ownership stake in foreign companies as a means to obtain controlled technology.<sup>51</sup> The fear that the Chinese government, if given the opportunity, would extend the use of this technology to collect communications is not an unreasonable fear. Two earlier CFIUS cases involving U.S. telecommunications service providers help put Global

---

47. See Jack Schafer, *Richard Perle Libel Watch, Week 3: Now he's playing defense*, SLATE MAGAZINE, Mar. 26, 2003, at <http://slate.msn.com/id/2080743>. See also Press Release, Office of U.S. Rep. Frank Wolf, Wolf Voices Concern about Proposed Sale of Global Crossing: Wants DOJ, State Department, DOD, Treasury and FCC to Fully Review Proposed Transaction (Apr. 9, 2003), at [http://www.house.gov/wolf/news/2003/04-09-Sale\\_Global\\_Crossing.html](http://www.house.gov/wolf/news/2003/04-09-Sale_Global_Crossing.html) [hereinafter Wolf Press Release] (Representative Wolf was Chairman of the House Commerce-Justice-State Appropriations Subcommittee when this was released).

48. Press Release, Global Crossing, Global Crossing Receives CFIUS Approval for ST Telemedia Investment (Sept. 19, 2003), available at <http://www.globalcrossing.com/xml/news/2003/september/19.xml>; Press Release, Global Crossing, ST Telemedia and Global Crossing Secure Final Regulatory Approval (Oct. 8, 2003), available at <http://www.globalcrossing.com/xml/news/2003/october/08.xml>.

49. "The FBI, CIA and the Pentagon had objected to the STT sale, arguing that the firm was too close to the Singaporean Government." *Global Crossing Sale Finally Agreed*, BBC NEWS, Oct. 9, 2003, at <http://news.bbc.co.uk/1/hi/business/3176630.stm>.

50. See Wolf Press Release, *supra* note 48.

51. "Computer-assisted analysis of China's exposed technology-related economic espionage activities in the United States reveals three basic operational patterns. . . . Second, American companies with access to the desired level of technology are purchased outright by Chinese state-run firms. . . ." *Terrorism and Intelligence Operations: Hearing Before the J. Economic Comm.*, 105th Cong. (1998) (statement of Nicholas Eftimiades), available at [http://www.fas.org/irp/congress/1998\\_hr/efimiad.htm](http://www.fas.org/irp/congress/1998_hr/efimiad.htm). See also PBS, *How China Spies*, at <http://www.pbs.org/wgbh/pages/frontline/shows/spy/spies/> (last visited May 9, 2005).

Crossing in perspective. A subsidiary of Nippon Telephone and Telegraph (“NTT”), which had the Japanese government as its majority shareholder at the time, was given permission to buy Verio, an Internet service provider, once FBI concerns about potential interference with its wiretapping efforts were resolved.<sup>52</sup> The DOJ and the FBI were concerned that Japanese law, which prohibits wiretapping of Japanese citizens (but which allows Japanese authorities to wiretap non-Japanese) could potentially complicate some criminal cases.<sup>53</sup> The FBI was concerned that Japanese entities could use NTT to gain access to information about surveillance efforts and technologies or information about U.S. customers.<sup>54</sup> The FBI also wanted assurance that Verio’s servers and data would remain in the United States and accessible to properly authorized law enforcement after the acquisition.<sup>55</sup>

The DOJ and the FBI, under the CFIUS framework, negotiated with NTT to obtain procedures that would protect sensitive information, make it easier for law enforcement officers to request information from Verio, and ensure that Verio customer information was not disclosed to unauthorized parties.<sup>56</sup> One part of the agreement, according to press reports, was that

---

52. “Less than two years ago, NTT paid a whopping \$5.5 billion for Verio, in a deal that had to be cleared by the Clinton administration after the FBI raised national-security issues.” Mark Lewis, *NTT Taking A Bath On Verio*, FORBES, Apr. 4, 2004, available at <http://www.forbes.com/2002/04/04/0404ntt.html>.

53. See Brian Quinton, *Welcome to America – almost. . .*, TELEPHONY ONLINE, Aug. 21, 2000, at [http://www.telephonyonline.com/ar/telecom\\_welcome\\_america\\_almost/index.html](http://www.telephonyonline.com/ar/telecom_welcome_america_almost/index.html).

54. “The Federal Bureau of Investigation, along with the Justice Department and the Pentagon, worries the deal could give the Japanese government-controlled company access to U.S. government wiretapping activity and could present an espionage risk.” Neil King Jr. & David S. Cloud, *U.S. Pushes to Resolve Debate on NTT-Verio*, WALL ST. J., Aug. 9, 2000, at A2–A14, available at <http://cryptome.org/verio-ntt-sec.htm> [hereinafter *U.S. Pushes to Resolve NTT Debate*].

“Even when the foreign entity controlling a U.S. communications network is privately held, there is cause for concern that the foreign-affiliated carrier may be subject to the influence and directives of the foreign government. . . .” *Foreign Government Ownership of American Telecommunications Companies: Before the Subcomm. on Telecomm., Trade, and Consumer Protection, House Comm. on Commerce*, 106th Cong. 43–47 (2000) (statement of Larry R. Parkinson, General Counsel, FBI) [hereinafter *Parkinson Statement on Foreign Government Ownership of Telecomm. Companies*].

“Within Japan, the Japanese government is believed to monitor all telecommunications traffic from U.S. corporations located in Japan.” PETER SCHWEIZER, *FRIENDLY SPIES: HOW AMERICA’S ALLIES ARE USING ECONOMIC ESPIONAGE TO STEAL OUR SECRETS* 18–19 (1993). See also JOHN J. FIALKA, *WAR BY OTHER MEANS: ECONOMIC ESPIONAGE IN AMERICA* 3–17 (1999).

55. Associated Press, *NTT-Verio Deal Sparks FBI concern*, CNET NEWS.COM (July 6, 2000), at <http://news.com.com/2100-1033-242823.html?legacy=cnet>.

56. *U.S. Pushes to Resolve NTT Debate*, supra note 55.

NTT would create a separate division within Verio staffed only by U.S. citizens who would be responsible for surveillance requests.<sup>57</sup> According to press reports, other FBI agreements also sought to restrict non-U.S. citizens' access to customers' billing and calling information.<sup>58</sup>

Deutsche Telekom's proposal to purchase VoiceStream Wireless created similar concerns. Deutsche Telekom's majority owner at the time of the case was the German government.<sup>59</sup> This led some in Congress to complain that the partial ownership by a foreign government would pose anticompetitive and national security issues.<sup>60</sup> CFIUS recommended that the acquisition be approved by the President after the FBI and Deutsche Telekom came to an agreement that assured the FBI that it would still be able to conduct wiretaps after the acquisition.<sup>61</sup>

In both of these cases, concerns over potential interference with U.S. law enforcement operations or with foreign access to U.S. communications led to investigation. These concerns were reinforced as the foreign acquirer in each case was partially owned by its home government, reflecting the movement toward privatization in the larger context of telecommunication liberalization. Access to U.S. communications and potential involvement of foreign governments also generated concern in the Global Crossing case.

There is anecdotal evidence for another case where a foreign telecommunications company that operated on a global basis had its acquisition of a U.S. company delayed by CFIUS, pending conclusion of a side agreement with U.S. agencies. The side agreement required the foreign company not only to cooperate with agencies in the United States, but also to cooperate with U.S. agencies in communication interceptions in a Caribbean country deeply involved in narcotics trafficking. According to company executives, these proposed extraterritorial requirements

---

57. "NTT was forced to create a separate division within Verio, staffed and run only by U.S. citizens, to work exclusively as the interface between the ISP and the FBI." Arik Hesseldahl, *Around-The-Globe: Federal Bureau Of Interference*, FORBES.COM, at <http://www.dotcomeon.com/fbi.html> (last visited May 9, 2005).

58. See Quinton, *supra* note 54; Neil King Jr. & David S. Cloud, *Hang Ups: Global Phone Deals Face Scrutiny From New Source: the FBI*, WALL ST. J., Aug. 24, 2000, at A1.

59. DEUTSCHE TELEKOM ANNUAL REPORT 2003, NOTES TO THE CONSOLIDATED FINANCIAL STATEMENTS: SUMMARY OF ACCOUNTING POLICIES, at <http://www.annualreport2003.telekom.de/site/en/ka/konzernanhang/index.php?tcfs=f6aa2b90e9348c5d8556eed72ff9dda5&c=1085212960>.

60. FCC approval was also required for the acquisition, but the FCC deferred to CFIUS in this case. See, e.g., Voicestream Wireless Corporation, Powertel Inc. Transferors, et al, *Separate Statement of Commissioner Harold Furchtgott-Roth*, 15 F.C.C.R. 3341, 3383 (2001), available at [http://www.fcc.gov/Speeches/Furchtgott\\_Roth/Statements/2001/sthfr130.pdf](http://www.fcc.gov/Speeches/Furchtgott_Roth/Statements/2001/sthfr130.pdf).

61. Arik Hesseldahl, *Around-The-Globe: Federal Bureau Of Interference*, FORBES, Dec. 20, 2000, available at <http://www.forbes.com/2000/12/20/1220atg.html>.

ultimately contributed to a decision by the foreign company to stop pursuing the acquisition.<sup>62</sup>

One of the new challenges for CFIUS is that ownership no longer adequately describes the range of potential foreign involvement in a communications network. The ranges of activities that create potential risks for security can be classified as Foreign Ownership, Control, or Influence (“FOCI”).<sup>63</sup> CFIUS authorities are not sufficient to cover actions that do not reach the level of ownership but which do provide a foreign entity with increased access and control. Consequently, the Committee and its authorities have come under renewed scrutiny.

Efforts to strengthen the CFIUS process in response to the perceived risks of foreign ownership of telecommunications service providers reflect the larger issue of the evolution of sovereignty in response to changes in the international economy. This evolution is likely to continue. Previous concepts of sovereignty and state authority included, if only by implication, an assumption of national ownership of critical industries. The national ownership gave governments an extra and informal measure of control and influence. This allowed them to assume a higher level of trust and security for the provision of critical goods and services. However, a focus on the country of origin provides an increasingly uncertain value toward mitigating risk.

### III. RISKS OF FOREIGN OWNERSHIP

The risk posed by foreign ownership is easy to overestimate, but it cannot be dismissed. The categories of risk are the following: damage to law enforcement interception capabilities, economic espionage, and the potential for damage to critical infrastructures. Of these categories, economic espionage is an increasing threat, because a number of countries engage in this activity and may use ownership of U.S. companies to aid their collection efforts.<sup>64</sup> The widely held suspicion that a few countries’ intelligence services—such as China’s or France’s—routinely exploit access to national telecommunications companies, where the government holds a stake for domestic intelligence purposes, makes it reasonable to assume that the same tactic might be attractive for foreign operations.

A key concept for assessing the risk is not whether foreign purchases increase the risk of economic espionage in some absolute sense, but

---

62. Based upon the Author’s interviews with company executives, who wished to remain anonymous.

63. DEPARTMENT OF DEFENSE OPERATING MANUAL, *supra* note 37.

64. JAMES LEWIS, GLOBALIZATION AND NATIONAL SECURITY: MAINTAINING U.S. TECHNOLOGICAL LEADERSHIP AND ECONOMIC STRENGTH 28–30 (2004).



whether they increase the risk relative to other potential avenues for the collection of economic intelligence. Prohibiting foreign ownership makes little sense if this ultimately does not degrade an opponent's ability to collect information. In this light, foreign purchases of U.S. telecommunications services probably do not greatly increase the risk of economic espionage, as there are many other avenues to collect information that work as well or better. Emplacing an agent as a foreign national employee in a U.S. firm or recruiting a U.S. citizen may be a cheaper and more effective approach.<sup>65</sup>

The risk to law enforcement intercept capabilities comes from three different sources: the blurring of jurisdiction, the potential for a foreign-owned company to be less cooperative than an American firm, and the possible clash of legal authorities. This clash of legal authorities arises in two different ways. First, the determination of when and against whom intercepts can be authorized, and second, the possibility that operational data might be stored outside the United States, thus becoming more difficult to reach under U.S. law. This clash of legal authorities is probably the greatest source of risk, since economics might impel a business to centralize data outside the United States in order to cut costs.

The clash of legal authorities is in part a problem of international law enforcement cooperation and harmonization of national laws, rather than of foreign ownership. Although there have been improvements since September 11, many procedures for law enforcement cooperation are still rooted in the stately pace of diplomacy in the early twentieth century and rely on Letters Rogatory<sup>66</sup> or bilateral Mutual Legal Assistance Treaties ("MLATs").<sup>67</sup> These treaties differ in scope from country to country and are difficult to negotiate because they raise complex sovereignty issues.<sup>68</sup>

---

65. See generally OFFICE OF THE NATIONAL COUNTERINTELLIGENCE EXECUTIVE, ANNUAL REPORT TO THE CONGRESS ON FOREIGN ECONOMIC COLLECTION AND INDUSTRIAL ESPIONAGE-2003 (Feb. 2004), available at [http://www.nacic.gov/publications/reports\\_speeches/reports/fecie\\_all/fecie\\_2003/fecie\\_2003.pdf](http://www.nacic.gov/publications/reports_speeches/reports/fecie_all/fecie_2003/fecie_2003.pdf).

66. "A letter rogatory is a formal request from a court in one country to 'the appropriate judicial authorities' in another country requesting service of process." PROCESS FORWARDING INTERNATIONAL, LETTERS ROGATORY, available at <http://www.hagueservice.net/lr.html> (last visited Apr. 21, 2005).

67. See BUREAU FOR INTERNATIONAL NARCOTICS AND LAW ENFORCEMENT, DEPARTMENT OF STATE, INTERNATIONAL NARCOTICS CONTROL STRATEGY REPORT (2004), available at <http://www.state.gov/g/inl/rls/nrcrpt/2003/vol2/html/29914.htm>; DEPARTMENT OF JUSTICE, U.S. ATTORNEYS MANUAL, Title 9, Section 276, available at [http://www.usdoj.gov/usao/eousa/foia\\_reading\\_room/usam/title9/text/t9rm02.wpd](http://www.usdoj.gov/usao/eousa/foia_reading_room/usam/title9/text/t9rm02.wpd) (last visited Apr. 20, 2005).

68. See James Lewis, *Strengthening Law Enforcement Capabilities to Combat Terrorism*, in TO PREVAIL: AN AMERICAN STRATEGY FOR THE CAMPAIGN AGAINST TERRORISM (2001), available at [http://www.csis.org/tech/strenght\\_law\\_enforce.pdf](http://www.csis.org/tech/strenght_law_enforce.pdf)

Strengthening existing MLATs and seeking broader multilateral arrangements could reduce the concern that foreign ownership might lead to a reduction in cooperation with law enforcement requests, but this is a long-term prospect, and in the interim the CFIUS process will continue to be used to meet law enforcement concerns.

The need to use CFIUS to ensure continued law enforcement access may become less pressing as national legal authorities for communications interception converge into common accepted international practices. In part this is the result of the need for increased cooperation that is required to respond to cybercrime.<sup>69</sup> Many countries either already possess more extensive legal access to communications than the United States, as with the United Kingdom or France, or are moving to bring their governmental enforcement power closer to U.S. practices, as with Japan.<sup>70</sup> Additionally, cooperation does not appear to be a problem since most companies, foreign or domestic, seem willing to help law enforcement and there are no reports to the contrary. The potential for a loss of confidentiality and the possibility of political constraints from foreign owners, however, do remain issues.

The primary issue for critical infrastructure protection is whether foreign ownership increases vulnerability. Vulnerability, in this regard, has two aspects: the ability to disrupt vital services and the ability to exploit ownership for greater access to communications. By estimating the risk created by scenarios where ownership can provide an advantage and then comparing these scenarios to alternatives, one can establish a metric for risk and vulnerability. In doing so, an initial conclusion could be that foreign ownership is only one source of vulnerability among many, and that its risks may be overstated.

Opportunity cost is an immediate consideration. There may be alternative approaches to either disruption or for communications interception that work as well without the cost of ownership. Discussion among the agencies that make up CFIUS has been broadened to consider FOCI in recognition that ownership is not the only, or even best, avenue for

---

(discussing sovereignty issues involved with MLATS).

69. See James K. Robinson, Remarks at the International Computer Crime Conference (May 29-31, 2000), at <http://www.usdoj.gov/criminal/cybercrime/roboslo.htm>; G8 Information Centre, Presidents Summary: Meeting of G8 Ministers of Justice and Home Affairs (May 5, 2003) at <http://www.g8.utoronto.ca/justice/justice030505.htm>.

70. *Wiretapping, numbering bills clear Diet in all-night session*, JAPAN TIMES, Aug. 12, 1999, available at <http://www.japantimes.com/cgi-bin/getarticle.pl5?nn19990812a1.htm>; Hiroshi Matsubara, *Wiretap Law: Hard to Use, Easy to Abuse*, JAPAN TIMES, Nov. 21, 2003, available at <http://www.japantimes.co.jp/cgi-bin/getarticle.pl5?nn20031121b3.htm>; Regulation of Investigatory Powers Act 2000, c. 23, Pt. I (Eng.), available at <http://www.hms0.gov.uk/acts/acts/2000/00023--b.htm>.

potential opponents to exploit the communications infrastructure.<sup>71</sup> In this context, risk may be high and vulnerability may increase, but foreign ownership is not the cause of this increase.

Access provided by ownership is not essential for communications interception. There may be an advantage to having direct access to business records, user information, and switches, but at best, this simplifies or shortens the time needed for these tasks. Physical access is valuable for interception of communications over fiber-optic networks, but it can also be obtained clandestinely rather than through purchase of the network. In general, the advantages provided by ownership can be duplicated by other techniques, such as recruiting company employees, forming partnerships, or having an agent gain employment with the target service provider. International telecommunications also involves complex partnering arrangements that could substitute in some areas for direct ownership.

The risk to critical infrastructure includes potential foreign access to communications for intelligence purposes, but also includes the potential for disruption of service. These activities, however, are unlikely categories of activity for terrorist groups. Al Qaeda, for example, is unlikely to purchase American telecommunications companies in order to gain the ability to disrupt the telephone services. The threat of service disruption lies elsewhere, with nations rather than subnational groups. Concern over foreign government access to information and infrastructure through the purchase of U.S. service providers is the primary motivation for increased scrutiny of foreign investment in U.S. companies.

If ownership is not in itself the sole factor for increasing the risks to telecommunications services, does this mean that CFIUS need not be reinforced? At a minimum, the limited increase in risk created by foreign ownership suggests that reinforcing regulatory oversight of transactions involving foreign purchasers is unlikely to materially reduce risk and vulnerability, particularly if oversight is greatly reduced once the transaction is completed. Potential opponents will adopt other methods that take advantage of increased economic integration to avoid CFIUS oversight. Another consideration is whether efforts to minimize the risks of foreign ownership, or alternative sources of risk such as foreign participation in the workforce or foreign technology suppliers, can be implemented without doing harm to the economy and long-term interests of the United States, where these interests outweigh any possible security benefit. These considerations alone justify a degree of caution in seeking new authorities.

---

71. *Parkinson Statement on Foreign Government Ownership of Telecomm. Companies*, *supra* note 54.

Ownership of infrastructure provides some advantages to a potential opponent, but is not critical for espionage or attacks on critical infrastructure. In some ways, the economic and technological changes that called attention to the risk of foreign ownership also acted to reduce that risk. While individual companies cannot afford the redundancy found in the old national monopoly systems,<sup>72</sup> the development of multiple service providers with multiple networks achieves a similar degree of security. Diversity of ownership and of telecommunications systems works against the possibility of a catastrophic attack and dilutes the risks of foreign ownership of the telecommunications infrastructure.

The risks from foreign ownership of U.S. telecommunications infrastructure are probably overstated, but one of the hallmarks of homeland security analysis in the United States is a willingness to adopt an exceptionally risk-averse approach to potential threats. Bureaucracies tend to be inherently risk-averse and the events of September 11 increased this tendency. While the probability of attacks on infrastructure by foreign owners is very low, the likelihood of attack does not shape regulations; instead, the potential damage that could arise if one of these improbable events were to occur shapes our regulations.

#### IV. NEW GOALS FOR REGULATION

U.S. policies generally encourage foreign investment in and ownership of American companies. Most of these acquisitions hold no risk for security. However, in the post-Cold War security environment—with concerns regarding economic espionage, critical infrastructure protection, and homeland security—support for foreign investment and ownership is no longer harmless.

Foreign investment is essential for the U.S. economy. In some circumstances, however, foreign investment also creates challenges for security, particularly if it involves access to, or control of, key infrastructures or advanced technologies. Previous concerns over technology transfer and economic espionage led to efforts strengthening the CFIUS process. In 1993, Congress amended Exon-Florio to require foreign, government-controlled companies to obtain CFIUS approval before acquiring U.S. companies when the foreign purchaser is “controlled by or acting on behalf of a foreign government” and the acquisition “could result in control of a person engaged in interstate commerce in the U.S. that

---

72. This pertains to old national monopoly system where the cost of redundant capabilities or hardened facilities could be passed on to all rate payers who did not have the option of switching to a lower cost provider.

could affect the national security of the United States.”<sup>73</sup> New and more restrictive policies proposed by the Department of Defense were not adopted.<sup>74</sup>

In the wake of Global Crossing, the U.S. government began to reconsider the process by which it reviews potential foreign acquisitions of U.S. companies. In particular, a review of the risks of foreign ownership of the telecommunications infrastructure commenced. Deregulation, the internationalization of economies, new technologies, and new kinds of threats guarantee that security agencies will continue to seek regulatory changes that, from their perspective, either reduce risk or preserve capabilities.

It is possible that these reviews will recommend expansion of federal oversight of foreign acquisitions, at least for foreign acquisitions of critical infrastructure. Critical infrastructure protection and the preservation of communications interception capabilities are goals of the CFIUS review process. In this sense, changes in CFIUS that better address transnational threats and communications interception risks would complement the changes in the Patriot Act and the Intelligence Reform and Terrorism Prevention Act to manage risk and maintain capabilities. Moving forward in adjusting to the new situation in telecommunications will require first an evolution in thinking about sovereignty and governmental authorities to accommodate an integrated international economy and second, the development of new authorities and techniques to lower risk and improve security.

Change is recurring and continuous for technology and economies. Changes in the authorities that govern and enable communications interception, at least in the United States, come in discontinuous clumps. This discontinuous process of mapping government authorities to the technological and business environment creates legitimate civil liberty and business concerns, which in themselves make the policy and regulatory process more complex and iterative when it comes to government action to preserve essential services.

---

73. *Exon-Florio Provision*, *supra* note 27 (citing 50 U.S.C. App. § 2170 (2002)).

74. 50 U.S.C. § 2170 (2000). Section 837(a) of the National Defense Authorization Act for Fiscal Year 1993 (the “Byrd Amendment”) amended Exon-Florio to require a CFIUS investigation when the acquiring company is controlled by or acting on behalf of a foreign government and the acquisition “could result in control of a person engaged in interstate commerce in the United States that could affect the national security of the United States.” § 2710(b). For the Department of Defense proposals, *see* JOINT SECURITY COMMISSION, REDEFINING SECURITY: A REPORT TO THE SECRETARY OF DEFENSE AND THE DIRECTOR OF CENTRAL INTELLIGENCE, ch. 6 (1994), at <http://www.loyola.edu/dept/politics/intel/jsc-report.pdf>.

The next set of changes in regulation will not be driven by technology, but by changes in the international economy and by new perceptions of risk. Efforts to strengthen the CFIUS process—in response to the perceived risks of foreign ownership of telecommunications service providers—reflect the larger issue of the evolution of sovereignty in response to changes in the international economy. This evolution is likely to continue. Previous concepts of sovereignty and state authority included, if only by implication, an assumption of national ownership of critical industries. This national ownership gave governments an extra and informal measure of control and influence and allowed them to assume a higher level of trust and security for the provision of critical goods and services. However, a focus on the country of ownership is increasingly of uncertain value for mitigating risk.