Under the Radar: NSA's Efforts to Secure Private-Sector Telecommunications Infrastructure

Susan Landau*

INTRODUCTION

When Google discovered that intruders were accessing certain Gmail accounts and stealing intellectual property,[1] the company turned to the National Security Agency (NSA) for help in securing its systems. For a company that had faced accusations of violating user privacy to ask for help from the agency that had been wiretapping Americans without warrants appeared decidedly odd, and Google came under a great deal of criticism. Google had approached a number of federal agencies for help on its problem; press reports focused on the company's approach to the NSA. Google's was the sensible approach. Not only was NSA the sole government agency with the necessary expertise to aid the company after its systems had been exploited, it was also the right agency to be doing so. That seems especially ironic in light of the recent revelations by Edward Snowden over the extent of NSA surveillance, including, apparently, Google inter-data-center communications.[2]

The NSA has always had two functions: the well-known one of signals intelligence, known in the trade as SIGINT, and the lesser known one of communications security or COMSEC. The former became the subject of novels, histories of the agency, and legend. The latter has garnered much less attention. One example of the myriad one could pick is David Kahn's seminal book on cryptography, *The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet*.[3] It devotes fifty pages to NSA and SIGINT and only ten pages to NSA and COMSEC. (The security of stored data also falls under NSA's purview; in this paper, my focus is securing data in transit.) In general, these COMSEC efforts flew under the radar.

Beginning somewhat before the agency's support of loosening U.S. cryptographic export-control regulations in the late 1990s, NSA's COMSEC side, the Information Assurance

* Professor of Cybersecurity Policy, Worcester Polytechnic Institute. This article was written while the author was a 2012 Guggenheim Fellow.

[1] David Drummond, *A New Approach to China*, GOOGLE POLICY BLOG (Jan. 12, 2010).

[2] Barton Gellman and Ashkan Soltani, *NSA Infiltrates Links to Yahoo, Google Centers Worldwide, Snowden Documents Say*, WASH. POST, Oct. 31, 2013.

[3] DAVID KAHN, THE CODEBREAKERS: THE COMPREHENSIVE HISTORY OF SECRET COMMUNICATION FROM ANCIENT TIMES TO THE INTERNET (rev. sub. ed. 1996).

Directorate (IAD), has quietly worked to improve the security—and then the privacy—of domestic communications infrastructure. These activities have been largely unnoticed by the public, which has instead been focused on NSA's warrantless wiretapping of domestic communications.[4] Nonetheless they are real, and they are particularly important in light of the cybersecurity and cyber-exploitation situation faced by virtually every nation.

For many, the role of the NSA as a securer of private-sector communications infrastructure is not only unexpected but actually counterintuitive, again because of the recent revelations in the documents leaked by Snowden.[5] Efforts to secure communications may well complicate legally authorized wiretaps. Yet NSA's recent efforts in protecting private-sector communications, and even communications infrastructure, are not only appropriate, but have some precedent. Even while the agency worked against securing private-sector communications from the 1980s through the mid 1990s, it sometimes helped secure some systems; during the 2000s, even while NSA promulgated a U.S. cryptographic algorithm that was insecure[6]—at least against NSA's SIGINT group—the agency also worked to provide secure communication systems to the public. These contradictory stances demonstrate how complex policy issues are in this domain.

In this paper I discuss NSA's recent, largely hidden, efforts to secure private-sector communications. Beginning in the mid-1990s, the NSA moved from delaying the deployment of cryptography in communications infrastructure to actively aiding the securing of domestic private-sector communications and communications infrastructure. Such security systems could also be used by targets of U.S. law enforcement and national intelligence, thus potentially complicating government investigations. Yet the NSA nonetheless viewed providing this technical guidance as the appropriate choice for national security. The rationale stemmed from two separate transformations that had their roots in the 1980s and accelerated through the 1990s and 2000s. The radical change in communications technologies and transformations in the communications industry was one cause; the other was the massive transformation in the U.S. Department of Defense's mission in the post–Cold War world. The combination meant that providing expertise so that the private sector could better secure communications became a national security priority. This was an untrumpeted shift, but a very real one.

I begin this unusual story by presenting the actions taken by the NSA to secure private-sector communications infrastructure over the last two decades. Next I examine the rationale behind NSA's efforts. I conclude by examining whether the efforts of the recent past can serve as a model for securing telecommunications infrastructure, or if some other policy solution will be needed.

---

[4] *See* James Risen and Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES, Dec. 16, 2005, at A1.

[5] *See The NSA Files*, THE GUARDIAN, http://www.guardian.co.uk/world/the-nsa-files.

[6] Nicole Perlroth, Jeff Larson, & Scott Shane, *NSA Able to Foil Basic Safeguards of Privacy on the Web*, N.Y. TIMES, Sept. 5, 2013, at A1. This revelation is also due to Snowden leaks.

Understanding the significance of NSA's actions requires understanding, at least at a rudimentary level, of telecommunications technology. Putting the NSA actions in context also requires some background in the conflict between the Department of Defense (DoD) and the Department of Commerce (DoC) for control of communications security, which I briefly discuss here.[7] I begin with a discussion on communications technology, then follow with a brief history reprising the NSA's role in securing private-sector communications. This falls naturally into three parts: the 1960s and 1970s, in which the NSA began playing a role in securing private-sector communications; the 1980s through the mid-1990s, when NSA sought control of private-sector communications security, and then the 1990s export-control battles over cryptography. With this history in place, I show how NSA has worked to secure private-sector communications infrastructure. I then discuss the rationale for this effort.

I. A BRIEF OVERVIEW OF COMMUNICATIONS SECURITY

No communications system is ever fully secure. A phone line can be tapped into, a key logger can be placed on a computer to capture the encryption key and transmit it to the interceptor—and even a trusted messenger can be intercepted. The latter was, of course, key to finding Osama bin Laden's hiding place in Abbottabad, which was determined by tracking his courier.[8]

In any attempt to conduct eavesdropping, the issue is what effort is necessary to be successful and what the likelihood is that the interception will be discovered. Under those parameters, for the first two-thirds of the twentieth century, U.S. private-sector communications were relatively secure from widespread interception, though not necessarily from targeted efforts.

The reason for this security lay in a combination of the business model for telecommunications and the type of technology employed. For most of the twentieth century, telephone service in the United States was largely synonymous with AT&T. The company's monopoly status meant that the company controlled all aspects of security for the Public Switched Telephone Network (PSTN). AT&T designed the phone switches; its subsidiary, Western Electric, developed the network devices—telephones—that ran on the network. (Before the 1968 "Carterfone" decision, no one else could even connect devices to the system.[9]) The phone company's switching equipment was large and weighty. It was protected from outside access through the physical security provided by telephone company central offices. Further security came from the fact that U.S. government communications traveled on the AT&T network. This meant both switching

[7] For the DoD–DoC conflict over civilian agency control of cryptography, see WHITFIELD DIFFIE & SUSAN LANDAU, PRIVACY ON THE LINE: THE POLITICS OF WIRETAPPING AND ENCRYPTION 66–85, 240–42 (updated and expanded ed. 2007).

[8] Mark Mazzeti, Helen Cooper, & Peter Baker, *Behind the Hunt for Bin Laden*, N.Y. TIMES, May 3, 2011, at A1.

[9] *See generally* Use of the Carterfone Device in Message Toll Telephone Service v. AT&T, 13 F.C.C.2d 420 (1968).

and transmission facilities had to be secured. Buried coaxial cable provided protection from interception. While such cables are, of course, tappable, doing so requires physical intrusion. It thus carries a certain amount of risk of being discovered. In contrast, tapping radio signals only requires an antenna, which can be easily hidden amongst antennas placed for legitimate purposes.[10]

Through the 1950s and 1960s, both the business and technology of telecommunications were relatively stable. Change, though, was in the air. One such was the use of microwave radio signals for transmitting telephone conversations. Cheaper to construct and install than telephone cables, microwave towers became the new transmission channel of choice. By the 1970s, 70% of AT&T's communications used microwave radio relays for transmission.[11] This decreased security. Because microwave signals spread out as they travel, all that is required to tap them is a receiver somewhere nearby, such as, on a roof of a nearby building.

From the point of view of communications security, the next significant change was the 1984 break-up of AT&T. This created a substantial increase in the number of communications providers. Many were small and undercapitalized, and thus unwilling to substantially invest in security.[12] Security was an investment that would not see an immediate rise in business; doing so was simply not worth it.

The rise of wireless communications occurred a short time later. With unprotected infrastructure and, at least initially, poorly protected communications, wireless was much less secure than the wireline communications systems that had preceded it. Indeed, in the beginning, communications between cell phones and base stations were not encrypted. Even today, the vast majority of cell towers lack minimal physical security.

The next significant change in communications security was the rise of the Internet and communications based on the Internet Protocol (IP). This has had a profound and quite negative impact on communications security. There are numerous reasons for the loss of security in moving communications to the Internet, not the least of which is the rich capabilities of the endpoint devices. But the fundamental reason for Internet communications insecurity arises from its mode of communication. While the Public Switched Telephone Network creates a dedicated circuit between callers on its network, communications using the Internet Protocol (IP) are broken into (small) packets that may in theory take different routes. IP communications combine control and content information in a single channel, and this change vastly simplifies the ability to attack the network and its users.

---

[10] Jeffrey Friedman, *TEMPEST: A Signal Problem*, NSA CRYPTOLOGIC SPECTRUM, Summer 1972, available at http://www.nsa.gov/public_info/_files/cryptologic_spectrum/tempest.pdf.

[11] *History of Network Transmission*, AT&T, http://www.corp.att.com/history/nethistory/transmission.html.

[12] There have always been very small local telecommunication carriers who did not invest in security; their size was such that their lack of security was not a serious issue. The ones I am speaking of here are substantially larger than these.

The recent changes to communications technologies have occurred against a backdrop of increasing global competition in everything from the production of telephone switches to the provision of services. The result is an increased need for communications security at the same time that service providers, both traditional communications providers and less traditional ISPs, lack resources. Until the recent leaks demonstrated the extent of NSA surveillance, there was also a marked lack of incentives; few customers demanded strong communications security. Google began standardly encrypting Gmail in only 2010 (this was after the discovery of intruders accessing user accounts).[13] Yahoo and Microsoft did not follow suit until the revelations in October 2013, which revealed the NSA had been intercepting the companies' inter–data-center communications.[14] If there were any remaining doubt regarding customers' lack of concern regarding communications security, just consider the decline of the Blackberry. This secure smartphone had 51% of the North American smartphone market in 2009, but security was not enough to keep its share of the marketplace.[15] The Blackberry lost out to competing products like the iPhone and Google's Android, far less secure, but with many more applications.

I now step back for a moment to describe how security was handled when telecommunications was technologically simpler.

II. 1960S AND 1970S: NSA DEVELOPS A ROLE IN SECURING PRIVATE-SECTOR COMMUNICATIONS

From its inception, the NSA has had a role in securing government communications. Because the government does not have its own communications network, it relies on private-sector transmission facilities. Thus the NSA's COMSEC mission includes ensuring the security of the private-sector transmission lines over which such government communications travel. In the technology world of the 1960s and 1970s, this meant ensuring the physical security of the switching offices and that transmissions were relatively resistant to interception. Such physical protections worked relatively well as long as communications traveled by copper wire.

With the development of microwave relay towers for telephone communications, the situation began to change. During the 1960s, the U.S. government became aware that the Soviets were intercepting microwave signals to spy on government communications. The Soviet embassy in Washington, a mere two blocks from the White House, was believed

---

[13] Ryan Singel, *Google Turns on Gmail Encryption to Protect Wi-Fi Users*, WIRED (Jan. 13, 2010), http://www.wired.com/threatlevel/2010/01/google-turns-on-gmail-encryption-to-protect-wi-fi-users/.

[14] *See* Brian Fung, *Even after NSA Revelations, Yahoo Won't Say If It Plans to Encrypt Data Center Traffic*, WASH. POST, Oct. 30 2013, http://www.washingtonpost.com/blogs/the-switch/wp/2013/10/30/even-after-nsa-revelations-yahoo-wont-say-if-it-plans-to-encrypt-data-center-traffic/; Craig Timberg, Barton Gellman, & Ashkan Soltani, *Microsoft Moves to Boost Security*, WASH. POST, Nov. 27, 2013, at A1.

[15] Robert Cozza, *SWOT: Research in Motion, Mobile Devices, Worldwide*, 5 GARTNER FOR BUSINESS LEADERS, May 29, 2009.

to be one source of the espionage, but there were multiple others, including even the use of cars in D.C.[16] President Ford directed that all critical government communications be routed on cables or wire lines until well out of the Washington area.[17]

Beginning in the early 1970s, Soviet interest expanded from U.S. military and diplomatic communications to communications of U.S. defense contractors.[18] The KGB sought surveillance against "scientific and technical targets" including Grumman, Fairchild, GE, IBM, Sperry Rand, and General Dynamics.[19] With an embassy two blocks from the White House, a UN mission in New York City, and a country house in Glen Cove, Long Island—and thus in close proximity to microwave towers along the Eastern Seaboard—the Soviets were well situated to tap into private-sector U.S. communications. And tap they did.

A government and defense contractor study in the early 1970s concluded the Soviets were indeed obtaining much useful information from eavesdropping on private-sector communications.[20] President Ford ordered communications security to "be extended to government defense contractors dealing in classified or sensitive information at the earliest possible time."[21] Ford ordered that communication circuits of defense contractors in Washington, New York, and San Francisco—the links most vulnerable to exploitation—be moved from microwave to cable and then, for the long term, the president sought nationwide secure domestic microwave communications.[22] NSA was placed in charge of developing the latter, but that control ended almost before it began. When Ford lost his bid for the presidency, the Carter administration, concerned about the potential for anti-competitiveness in the Ford plan (smaller telecommunications firms could not afford, as AT&T could, to use the buried cable solution), the antitrust case that the government was pursuing against AT&T, and the sheer cost that securing communications infrastructure (at the time, estimated to be $1–$2 billion), was quite hesitant about putting the Department of Defense in control over private-sector communications.[23] Instead of emphasizing securing communications infrastructure, the administration focused on securing defense contractors.

The new plan was for secure telephones. This became the NSA STU series. The first two STU systems were not exactly "user friendly." The STU-1 cost $35,000 , a hefty price in the late 1970s. While the STU-II cost half of that, it used centralized key management for

---

[16] Thomas R. Johnson, *American Cryptology During the Cold War, 1945–1989; Book III: Retrenchment and Reform: 1972–1980*, *in* 5 UNITED STATES CRYPTOLOGIC HISTORY 144 (National Security Agency: Center for Cryptological History, 1998).
[17] Memorandum from Henry Kissinger to the Sec. of Def., *National Security Defense Memorandum 266* (Aug. 15, 1974).
[18] *See* Johnson, *supra* note 16, at 145.
[19] *Id.*
[20] *Id.* at 148.
[21] Memorandum from Brent Scowcroft to the Sec. of Def. and Dir. Of the Office of Telecomm. Policy, *National Security Memorandum 338* (Sept. 1, 1976).
[22] *Id.* at 2.
[23] *See* Johnson, *supra* note 16, at 146–49.

all contacts, making communication extremely slow. According to an NSA history, "even people having the instruments would use them only when they had plenty of time or were certain they would get into classified material during the call."[24] The STU-III, introduced in 1987, was much more popular, and sold in the hundreds of thousands.

Even though the NSA of the 1970s and 1980s was kept out of securing private-sector communications, the agency would occasionally directly intervene with the private sector as it became aware of problems. In the 1970s, the agency told IBM, whose main offices lay across Long Island Sound from a Soviet "dacha" in Glen Cove, that Soviet intelligence agents were systematically eavesdropping on conversations between executives on the company's private microwave network.[25] In the 1980s, the government informed another U.S. company that its microwave communications were vulnerable. The government had uncovered others listening in.[26] A number of other situations in which the NSA informed private enterprise of security problems with communications infrastructure also occurred.

Yet while the NSA could and, in rare episodes, did warn the private sector about electronic eavesdropping, this was not actually an agency role. With the exception of the development of the STU systems, whose use was limited to the government and defense contractors, NSA was not directly involved in securing private-sector communications. Indeed, while the NSA is responsible for ensuring the security of national security communications systems, with rare exceptions the NSA does not do the same for the non–national security systems. This is a matter of budgetary issues rather than legislative prohibition. That said, in the 1980s and 1990s, there was a large battle over whether NSA's role should extend to securing private-sector communications infrastructure.

The 1970s saw the arrival of cryptography developed by the private sector. In the decades immediately after World War II, cryptography research was largely limited to the NSA. But by the 1970s, driven by the impending arrival of computers for use in day-to-day consumer interactions, private industry began work in the area of secure systems, including cryptography.

In 1973, in response to the federal government's need to securely store civilian data it was collecting, NIST[27] requested submissions of an algorithm for securing sensitive unclassified information. Only IBM responded. NIST had organized the effort of finding a data encryption standard, but the only government agency that had the capability to

[24] *Id.* at 150.
[25] SUSAN LANDAU, STEPHEN KENT, CLINTON BROOKS, SCOTT CHARNEY, DOROTHY DENNING, WHITFIELD DIFFIE, ANTHONY LAUCK, DOUGLAS MILLER, PETER NEUMANN, & DAVID SOBEL, CODES, KEYS, AND CONFLICTS: ISSUES IN U.S. CRYPTO POLICY: REPORT OF A SPECIAL PANEL ON THE ACM U.S. PUBLIC POLICY COMMITTEE 1 (June 1994).
[26] Comm. To Study Nat'l Cryptography Policy, Nat' Research Council, Cryptography's Role in Securing the Information Society 68 (Kenneth W. Dam & Herbert S. Lin, eds., 1996).
[27] At the time, NIST was the National Bureau of Standards; it became the National Institute of Standards and Technology, or NIST, in 1988. For simplicity, throughout this paper I will refer to the organization as the National Institute of Standards and Technology or NIST.

evaluate the algorithm was the NSA, which did so. A modified version of IBM's submission became the Data Encryption Standard (DES), a Federal Information Processing Standard (FIPS). While seemingly an arcane and technical issue, designation as a FIPS affects whether the algorithm or protocol must be in systems sold to the U.S. government or contractors. This can also affect much broader industry and international acceptance.

A lack of transparency in the DES selection process gave rise to doubts about the algorithm's strength. An encryption algorithm is considered strong if it is difficult to decrypt given current technology. Encrypted material should remain secure for some reasonable amount of time; how long this should be will vary by application. So while a command in the field might need to be secure only for a matter of hours, stored health records might require being secure for a quarter of a century.[28]

If an encryption algorithm is properly designed, then the algorithm's strength is based on the number of key bits; in the absence of a key, increasing the key length by a single digit doubles the time needed for a brute-force effort of decrypting. While an earlier IBM design had a key size of 64 bits, DES as finally accepted by NIST was 56 bits. Why the shrinkage? A now–partially declassified NSA history states that "they compromised on a 56-bit key."[29] The "they" is presumably IBM and the NSA.

Many believed that DES's design and short key size made the algorithm potentially breakable by the NSA, but in fact, the algorithm has stood the test of time. A research paper published in the early 1990s showed that DES had been designed to be secure against attacks known by IBM and the NSA in 1975 but not yet public at the time of the algorithm's debut.[30] It was not until July 1998 that a brute-force attack searching for all possible keys was able to break the DES. The machine to do the decryption was a special-purpose device using custom-designed chips and a personal computer built for less than $250,000, a price well within reach of criminal groups—not to mention nation states.[31]

The DES was not the only striking cryptographic development of the 1970s. Anticipating Internet commerce, two Stanford University researchers, Whitfield Diffie and Martin Hellman, and a University of California graduate student, Ralph Merkle, invented public-key cryptography, a system in which a widely known key, the public key, is used to

[28] Note that that quarter of a century might be after the algorithm has already been in use for some time. Thus, the encrypted material must be secure for twenty-five years—fifteen years after the algorithm's introduction. This means that the algorithm's security must be good for close to forty years from its initial fielding.
[29] Johnson, *supra* note 16, at 232.
[30] Don Coppersmith, *The Data Encryption Standard (DES) and Its Strength Against Attacks*, 38 IBM J. RES. & DEV. 243 (1994).
[31] *See* ELECTRONIC FRONTIER FOUNDATION, CRACKING DES: SECRETS OF ENCRYPTION RESEARCH, WIRETAP POLITICS, & CHIP DESIGN (1998). The attackers were somewhat lucky, as the key was discovered after only a quarter of the key space was searched instead of the expected half.

encrypt communications; a private key, held by the recipient, enables decryption.[32] Because of the complexity of inverting the encrypting method, knowing how to encrypt—that is, knowing the public key—does not aid in decryption. This means two users who have never communicated with one another are able to exchange keying information in such a way that an eavesdropper to their communications cannot decrypt their subsequently encrypted messages. Diffie and Hellman also invented digital signatures, a technique that enables an entity such as a bank, an individual, or a company to "sign" communications in such a way that the receiver can be sure of the sender's identity. This means of authentication is critical to a digital economy.

The Diffie-Hellman method provides a way of sharing keys, but is not itself an encryption technique. In 1977, MIT faculty Ronald Rivest, Adi Shamir, and Leonard Adleman developed the RSA public-key system for both encryption and digital signatures.[33] The RSA digital-signature scheme is a variant of RSA encryption.

Cryptography can serve many purposes in security. The well-known use is to provide confidentiality, ensuring that only the intended recipients of a communication could understand. But cryptography can also provide authenticity of the communication, by mathematically ensuring that the sender is who he claims to be, as well as integrity checking, mathematically ensuring that a received communication has not been altered in transmission. All three services are necessary for security in a networked environment.

Widespread adoption of these cryptographic techniques into communications systems took several decades. Much of the reason was that the killer apps — features or applications of a new technology that make the technology virtually indispensable — were financial transactions on the Internet and, later, on mobile communications. These only really began to take off in the mid 1990s when the Internet became commercialized. But the other reason for slow adoption was the government, which did not oppose the use of cryptography for authentication and integrity checking, but strongly opposed its use *outside the government* for confidentiality purposes. The 1980s and 1990s saw a very public battle over the use of cryptography by the private sector—the "Crypto Wars."

III. THE 1980S AND 1990S: WHO CONTROLS COMMUNICATIONS SECURITY—COMMERCE OR THE NSA?

In 1967 Congress passed the Brooks Act placing the secretary of commerce in charge of making recommendations for standards for computer equipment purchased by the federal government. As the National Bureau of Standards—later to become the National Institute of Standards and Technology (NIST)—was already in charge of determining many types of standards, the 1967 act was completely non-controversial. The law, however, meant

[32] Whitfield Diffie & Martin E. Hellman, *New Directions in Cryptography*, IT-22 IEEE TRANSACTIONS ON INFO. THEORY 644 (1976).
[33] Ronald L. Rivest, Adi Shamir & Leonard Adleman, *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*, 21 COMM. OF THE ACM 120 (1978).

that Congress, and especially Representative Jack Brooks, for whom the bill was named, now had some skin in the game.

In handling the issue of foreign government interception of the communications of U.S. industry, the Carter administration preference was to involve the Department of Commerce, rather than the Department of Defense.[34] The Reagan administration saw the situation differently. Concerned about the potential for espionage in government and contractor computer systems, in September 1984, the administration issued National Security Decision Directive 145,[35] placing the Department of Defense in charge not only of securing their own system, but also those of DoD contractors, including those not involved in secret work. This created a real flashpoint. NSA tried hard to explain its efforts were only advisory;[36] the contractors said otherwise.[37]

The White House sought an NSA role of developing cybersecurity for the private sector. Congress did not concur. In 1987 Congress passed the Computer Security Act. The passage of the act was quite controversial, and various issues were at play. The administration did not want Admiral John Poindexter, who had written NSDD 145, to testify. Poindexter had been involved in the Iran-Contra scandal, and testifying on NSDD-145 might open the door to turn questions onto other topics.

The Computer Security Act made NIST responsible for developing security standards for non–national security systems, assigning the agency "responsibility for developing standards and guidelines for Federal computer systems, including responsibility for developing standards and guidelines needed to ensure the cost-effective security and privacy of sensitive information in Federal computer systems, *drawing on the technical advice and assistance (including work products) of the National Security Agency, where appropriate*".[38] The issue, of course, was how the "technical advice and assistance" would be handled.

NSA saw the "technical advice" it was supposed to supply to NIST as a potential opportunity to regain the control it had lost both through the Computer Security Act as well as through an increasingly robust private-sector cryptographic research community. In 1989 NIST and the NSA signed a Memorandum of Understanding (MOU) governing their cooperation. The MOU established a six-person technical working group "to review

[34] *See Presidential Directive NSC-24, Telecommunications Protection Policy* 4 (Nov. 16, 1977, rev'd, Feb. 9, 1979).
[35] White House, *National Security Division Directive 145—National Policy on Telecommunications and Automated Information Systems Security* (Sept. 17, 1984).
[36] Hearings to Consider H.R. 145, the Computer Security Act of 1987, to Amend the Federal Property and Administrative Services Act of 1949 Brooks Act to improve Federal Computer Systems Security Before the Subcomm. on Legislation and National Security of the H. Comm. on Oversight & Gov't Reform 100th Cong. 281 (1987) (statement of Lt. Gen. William Odom, Dir. Of the Nat'l Sec. Agency).
[37] Hearings to Consider H.R. 145, the Computer Security Act of 1987, to Amend the Federal Property and Administrative Services Act of 1949 Brooks Act to improve Federal Computer Systems Security Before the Subcomm. on Legislation and Nat'l Sec. of the H. Comm. on Oversight & Gov't Reform 100th Cong. 281 (1987).
[38] Computer Security Act of 1987, Pub. L. No. 100-235, § 2(b), 101 Stat. 1724 (1988) (emphasis added).

and analyze issues . . . pertinent to protection of systems that process sensitive or other unclassified information."[39] Three members were to be from NSA, three from NIST, and output from the Technical Working Group (TWG) was to be reviewed by both the NSA and NIST prior to public release. Controversial issues could be elevated to the secretary of defense and the secretary of commerce—or even the president—a seeming transfer of power to the NSA given the responsibilities that the Computer Security Act had given to NIST. The TWG structure appeared to put NSA in the driver's seat.

The first issue facing the TWG was the designation of a digital-signature standard. Minutes of the Technical Working Group meetings demonstrate NIST members pushing for approval of a public-key-based digital-signature standard quickly, and NSA members of the group creating delays.[40] The issue was the RSA digital-signature algorithm, which NIST sought to make a FIPS. Because RSA digital signatures and RSA encryption use the same underlying cryptographic algorithm, approving the RSA digital-signature standard as a FIPS would have the effect of broadening use of the RSA encryption algorithm. NSA did not want this to occur.

The TWG meetings began in May 1989 with NIST presenting an algorithm on which they wanted to standardize. Instead NSA worked to block the RSA digital-signature algorithm from becoming a FIPS. While a FIPS designation simply means a standard for use in U.S. government computer systems, such a designation often results in broad acceptance internationally by governments and industry standards groups, and can lead to wide deployment.

NSA developed a new set of criteria for a digital-signature standard. Nine months later

[39] Memorandum of Understanding Between the Director of the National Institute of Standards and Technology and the Director of the National Security Agency Concerning the Implementation of Public Law 100-235 (Mar. 23, 1989).

[40] At the initial meeting on May 5, 1989, NIST members made clear they would like public-key standards, including digital-signature standards, out quickly: "NIST plans to develop the necessary public-key based security standards. We require a public-key algorithm for calculating digital signatures and we also require a public-key algorithm for distributing secret keys . . . We would prefer having one public key (asymmetric) cryptographic algorithm that does both digital signatures and key distribution. We would like NSA to assist this standards program by evaluating candidate algorithms proposed by NIST and *by providing new algorithms when existing algorithms do not meet NIST requirements.*" TWG Issue Number 1 (May 5, 1989), *in* THE THIRD CPSR CRYPTOGRAPHY AND PRIVACY CONFERENCE: SOURCEBOOK (David Banisar, Marc Rotenberg & Computer Professionals for Social Responsibility eds., 1993) (emphasis added). At the next meeting a week later, NSA's response was that it would assist in finding "the best solution to the problem." Memorandum for the Record, Second Meeting of the NIST/NSA Technical Working Group (May 13, 1989), *in* THE THIRD CPSR CRYPTOGRAPHY AND PRIVACY CONFERENCE: SOURCEBOOK (David Banisar, Marc Rotenberg & Computer Professionals for Social Responsibility eds., 1993). By May 23, 1989, less than a month after the joint effort had started, NIST members began discussing the TWG collaboration using terms such as "slippage" and "continuing delays" to describe the situation. Memorandum for the Record, Ninth Meeting of the NIST/NSA Technical Working Group (Nov. 23, 1989), *in* THE THIRD CPSR CRYPTOGRAPHY AND PRIVACY CONFERENCE: SOURCEBOOK (David Banisar, Marc Rotenberg & Computer Professionals for Social Responsibility eds., 1993).

they produced a classified digital-signature algorithm they would shortly declassify.[41] The NSA algorithm satisfied NSA criteria—but not NIST's. Even though NIST had presented a proposal for a digital-signature standard at the initial TWG meeting, twenty-one months of TWG meetings had not produced a standard.[42] That was not the only problem with the NSA candidate. The standard as originally proposed used too small a key size for the signature to actually be secure.

Other serious trouble soon surfaced. In April 1993, the *New York Times* reported on an NSA-designed cryptosystem for telephone conversations.[43] Called "Clipper" after its encryption chip, the system used secret encryption keys that were to be split and escrowed by two (as yet unspecified) government agencies. Law enforcement would be able to access the keys under court order.[44] Seeking broad use of the system, the Clinton administration intended to make the NSA-designed system a FIPS. In seeking to do so, NIST was serving as a "laundering" mechanism for the NSA effort.

It is hard to imagine a more negative reception to Clipper than the one that ensued. An announcement of the proposed standard in the Federal Register generated 320 comments, almost all of them negative. Among these were some from government agencies; the Department of Energy, the U.S. Agency for International Development, and the Nuclear

---

[41] "The first, classified CONFIDENTIAL, contained NSA's proposal to NIST containing a cryptographic algorithm and a hashing function which can be used as bases for an unclassified standard for digital signatures used by the U.S. Government. The document presents the results of the technical investigation of public key cryptographic algorithms conducted by NSA pursuant to the NIST request of May 5, 1989. [XXX] stated that it is NSA's intent to promptly initiate declassification action on this document." Memorandum for the Record, Fifteenth Meeting of the NIST/NSA Technical Working Group (Mar. 26, 1990), *in* THE THIRD CPSR CRYPTOGRAPHY AND PRIVACY CONFERENCE: SOURCEBOOK (David Banisar, Marc Rotenberg & Computer Professionals for Social Responsibility eds., 1993) (minutes are mistakenly dated "1989").
The NSA's candidate for the Digital Signature Standard was an in-house algorithm very similar to one already patented in the U.S. and Europe. That was not the only problem with the NSA candidate. The original proposed standard used too small a key size for the signature to be secure. Brian A. LaMacchia & Andrew Odlyzko, *Computation of Discrete Logarithms in Prime Fields*, 1 DESIGN, CODES, AND CRYPTOGRAPHY 47 (1991); DIFFIE & LANDAU, *supra* note 7. After including a flexible key size that enabled far greater security, the Digital Signature Standard proposed by NSA was approved by NIST as a Federal Information Processing Standard (FIPS). Federal Information Processing Standards Pub. No. 186, Digital Signature Standard (effective Dec. 1, 1994); 59 Fed. Reg. 26.208 (1994).

[42] In July 1990, NIST members said, "We're not getting anywhere; these issues aren't technical, they're policy. The NIST/NSA Technical Working Group (TWG) has held 18 meetings over the past 13 months. A part of every meeting has focused on the NIST intent to develop a Public Key Standard Algorithm Standard. We are convinced that the TWG process has reached a point where continuing discussions of the public key issue will yield only marginal results. Simply stated, we believe that over the past 13 months we have explored the technical and national security equity issues to the point where a decision is required on the future direction of digital signature standard." Memorandum from Dennis K. Branstad & F. Lynn McNulty to John W. Lyons, Director NIST (July 1990), *in* THE THIRD CPSR CRYPTOGRAPHY AND PRIVACY CONFERENCE: SOURCEBOOK (David Banisar, Marc Rotenberg & Computer Professionals for Social Responsibility eds., 1993).

[43] John Markoff, *Electronics Plan Aims to Balance Government Access with Privacy*, N.Y. TIMES, Apr. 16, 1993, at A1.

[44] John Markoff, *Communication Plan Draws Mixed Reaction*, N.Y. TIMES, Apr. 17, 1993, at 1.

Regulatory Commission all submitted letters to NIST opposing adoption of the Clipper standard. The Computer System Security and Privacy Advisory Board, a NIST-appointed federal advisory committee, passed several resolutions quite critical of the effort.[45] Concerns included the costs of the technology and the difficulty of marketing Clipper products abroad.[46] The board noted that the technology did "not address the needs of the software industry,"[47] a relatively mild reproof given the strong industry objections to the key-escrow system.

The real showdown occurred in the marketplace. Few sales took place. The FBI bought nine thousand Clipper-enabled telephones to seed the market; fewer than eight thousand other Clipper-enabled phones were sold, most to buyers in Venezuela and several Middle Eastern nations.[48]

Clipper's main impact, however, may have been its galvanization of the Crypto Wars,[49] the conflict between the government on the one hand, and industry and academia, on the other. On the cusp of the Internet era, industry pressed for the ability to secure systems through the widespread use of strong cryptography; the government resisted. The battles centered on export controls.

The U.S. government, seeking to prevent the deployment of cryptography for confidentiality purposes, used export controls to accomplish its goal. That export controls could have an impact on domestic use was the result of several factors. The first was the unwillingness of end users—at the time, mostly corporations—to use cryptography as a stand-alone product, preferring instead that it be incorporated within a system. While the controls applied only to products intended for overseas, hardware and software manufacturers found the situation of selling systems with weak forms of encryption abroad and strong ones domestically unpalatable. The result: U.S. hardware and software companies eschewed the use of strong cryptography.

In the 1990s, industry pushed back against the government controls. Progress was slow at first. For example, a 1992 agreement between NSA and RSA Data Security, a leading supplier of cryptographic software, on an expedited export approval process for systems with relatively short key length. The key length was 40 bits; at the time this was breakable by a personal computer in about a month, through a simple brute-force search. Late in the decade, Congress entered the fray largely supporting industry. Several bills simplifying the export of products with strong cryptography made their way to the

[45] *See* Computer System Security and Privacy Advisory Board, *Attachment to Resolution #1*, June 4, 1993; Computer System Security and Privacy Advisory Board, *Resolution #2*, June 4, 1993; Computer System Security and Privacy Advisory Board, *Resolution 93-5*, Sept. 1–2, 1993.
[46] Computer System Security and Privacy Advisory Board, *Resolution 93-5*, Sept. 1–2, 1993.
[47] *Id.*
[48] Communication between Whitfield Diffie and AT&T personnel (on file with Diffie).
[49] STEPHEN LEVY, CRYPTO: HOW THE CODE WARRIORS BEAT THE GOVERNMENT—SAVING PRIVACY IN THE DIGITAL AGE (2001).

floor.[50] They might have gone further but for FBI Director Louis Freeh.[51]

The FBI had entered the Crypto Wars after an intervention of the NSA. Following the passage of the Computer Security Act, NSA and NIST sought to inform the bureau of the impact of changing communications technologies.[52] This took some effort. But once the bureau grasped the threat digital communications and encryption posed to wiretapping, it moved into action. One direction was the 1994 Communications Assistance for Law Enforcement Act (CALEA),[53] a controversial law that requires all digitally switched networks be built wiretap accessible. The FBI evinced strong support for key escrow. In line with the NSA position, the FBI strongly opposed wide deployment of strong cryptographic systems.[54]

The FBI's opposition to strong cryptography created a new dynamic in the public discussion of communications security. Up until now, the NSA had been the only agency fighting the Crypto Wars. Now it had a domestic partner that could be much more public about the issue. The FBI could—and did—bring in such domestic concerns as kidnappings in its fight against encryption.[55] This was regardless of the role that encryption played in such investigations.[56] In many ways, the FBI was the more vociferous of the two agencies in objecting to society's broader use of cryptography.

Yet even as the FBI director pressed on the dangers of unbridled use of cryptography, other influential groups saw the situation of securing communications differently. In 1993 the administration had pressed for the certification of Clipper as a FIPS. By 1996, a report issued by the National Research Council determined, "On balance, the advantages of more widespread use of cryptography outweigh the disadvantages."[57] As the Internet grew in importance as an economic force, the ability to secure financial transactions

---

[50] Amy Branson, *Encryption Legislation at a Glance*, WASH. POST, Apr. 24, 1998, http://www.washingtonpost.com/wp-srv/politics/special/encryption/legislation.htm.
[51] *Id.*
[52] DIFFIE & LANDAU, *supra* note 7, at 83–85.
[53] Communications Assistance for Law Enforcement Act, 47 U.S.C. § 229 (1994).
[54] The FBI statements opposing widespread deployment of strong encryption appeared in many places, including a 1992 memo by National Security Advisor Brent Scowcroft, a September 1994 statement by FBI Director Freeh while attending a conference on Global Cryptography in Washington, and a statement by Director Freeh at hearings of the Senate Committee on Commerce, Science, and Transportation on July 25, 1996. The White House said these were FBI statements, not administration policy.
[55] *Enforcement of Federal Drug Laws: Strategies and Policies of the FBI and DEA: Hearing Before the H. Comm. on the Judiciary*, 104th Cong. D449-D451 (1995) (statement of Louis Freeh, Director, Federal Bureau of Investigation).
[56] In fact, content wiretaps play a minimal role in kidnappings. This is due to a number of factors, including the fact that the police typically don't know who the kidnappers are—and thus can't wiretap them. DIFFIE & LANDAU, *supra* note 7, at 211. Nearly two decades after the FBI began fighting to prevent the wide deployment of encryption, the technology still has yet to seriously impede criminal wiretaps. Because of Public Law 106-197, the annual Wiretap Report issued by the Administrative Office of the U.S. Courts reports on the number of times encryption is encountered during wiretaps. While there were a number of state cases reported between 2000–2011 (the last date for which information is available), only one proved impossible to decrypt.
[57] Dam & Lin, *supra* note 26, at 6.

became crucial. Pressures to change the cryptographic export controls grew, and the NSA became concerned about Congress. If cryptographic export controls were to change, the agency preferred that this occur through modifying regulations under the administration's control than by legislation. Carefully constructed regulations would be less damaging to NSA's interests than would be a broadbrush approach from Congress.

There was an additional set of issues at hand. NSA's famed ability to decrypt communications was running into the new reality of increased strength of cryptosystems—and a consequent decreased capability for the agency to read communications.[58] The increased use of fiber-optic cables also impeded collection. This combination made network exploitation—using computer networks to gather intelligence and to infiltrate target computers to gather intelligence—a high priority for the agency. NSA's backing down on cryptographic export control gave the agency a bargaining tool for increased funding in network exploitation, the agency's new emphasis.

By the end of the 1990s, the NSA acknowledged the time had come to allow public use of strong encryption systems. In early 2000, the White House announced substantial changes to the cryptographic export-control regime. Regardless of key length, cryptography for retail purposes—high-volume non-custom items—would not be controlled. Depending on the customer, other items would require licenses; there were more stringent requirements if the customer was a government.[59] The new rules gave the industry much of what it wanted, while still preserving controls on equipment sold to governments and communications providers. There were no controls if the item was retail, which meant it was sold widely and in large volume, freely available, not tailored for individual customers nor extensively supported post-sale, and not explicitly intended for protecting communications infrastructure. Industry opposition ended. So did congressional attempts to modify the cryptographic export-control regime.

With the agency now supporting a loosening of the cryptographic export controls, NSA and FBI interests had diverged. While the NSA was quite comfortable with the changes, which would have a major impact on the domestic use of encryption, the FBI was not.[60] Though their differences were never aired in public, after the change in export-control regulations, various subsequent efforts by the FBI to control the use of cryptography in securing communications did not appear to receive NSA support. In September 2010, the FBI floated the idea of controls on encryption.[61] The agency later backed away from this;[62] as of three-and-a-half years later, there has been no support from the Department of Defense on this aspect of the "Going Dark" plan.

---

[58] Seymour M. Hersh, *Annals of National Security: The Intelligence Gap*, THE NEW YORKER, Dec. 6, 1999, at 58.
[59] Revisions to Encryption Items, 15 C.F.R. §§ 734, 740, 742, 770, 772, and 774.
[60] Charlie Savage, *U.S. Tries to Make It Easier to Wiretap the Internet*, N.Y. TIMES, Sept. 27, 2010, at A1.
[61] *Id.*
[62] *Going Dark: Lawful Electronic Surveillance in the Face of New Technologies*: *Hearing Before the Subcomm. on Crime, Terrorism, and Homeland Security of the H. Comm. on the Judiciary*, 112th Cong. (2011) (statement of Valerie Caproni, General Counsel, Federal Bureau of Investigation).

IV. LATE 1990S TO THE PRESENT: MAJOR CHANGE HIDDEN IN PLAIN SIGHT

Even before the administration's about-face on cryptographic export controls, NSA behavior toward private-sector communications security was shifting. The first public hint occurred at a standards meeting, one that concerned certifying the protocols for elliptic-curve cryptography (ECC). Standards are a critical step in making the transition from a purely mathematical algorithm to an implementable protocol; in order for ECC to actually be used for securing communications, the protocol had to be certified by a standards body such as the American National Standards Institute (ANSI).

ECC was a second-generation public-key system invented independently by Neal Koblitz and Victor Miller in 1985. The algorithm's claim to fame is efficiency. For the same level of security as an RSA system, ECC-encrypted systems require a key size approximately a tenth the size of an RSA-system.[63] This means that an ECC-encrypted device requires significantly less storage and power than a device using RSA, and gave ECC a distinct advantage in securing low-powered small memory devices, such as early cellphones. It made ECC a potential business threat to systems using RSA. At a 1995 ANSI meeting, proponents of elliptic-curve cryptosystems (ECC) were clashing with employees of RSA Data Security, the company building security systems based on RSA. Koblitz et al. later described the situation:

> Meetings of standards bodies typically include industry representatives who have little mathematical background and so are easily manipulated by scare tactics. At the meeting in question, the RSA people were casting doubt on the safety of ECC-based protocols. As the heated debate continued, one of the NSA representatives left to make a phone call. He then returned to the meeting and announced that NSA believed that ECC had sufficient security to be used for communications among all U.S. government agencies, including the Federal Reserve. People were stunned. Normally the NSA representatives at standards meetings would sit quietly and hardly say a word. No one had expected such a direct and unambiguous statement from NSA—a statement that tipped the scales at ANSI in favor of ECC.[64]

[63] There are some caveats to this statement, which is not entirely precise. As key length increases, the relative advantage of the ECC algorithm increases. The relationship of "one-tenth" holds at the RSA 1024-bit key length; at smaller key sizes, ECC key sizes are somewhat larger than a tenth RSA key sizes for the same strength cryptosystem; at over RSA 1024-bit key length, ECC key sizes are somewhat smaller than a tenth. *See, e.g.*, ELAINE BARKER, WILLIAM BARKER, WILLIAM BURR, WILLIAM POLK & MILES SMID, COMPUTER SECURITY DIVISION, INFORMATION TECHNOLOGY LABORATORY, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, COMPUTER SECURITY: RECOMMENDATION FOR KEY MANAGEMENT – PART 1: GENERAL (REVISION 3) 64 (2012).

[64] Ann Hibner Koblitz, Neal Koblitz & Alfred Menezes, *Elliptic Curve Cryptography: The Serpentine Course of a Paradigm Shift*, 131 J. OF NUMBER THEORY 781, 781-814 (2011).

Making such a public statement about a non-governmental algorithm was very unusual for the NSA. Another came in the form of the TWG. At first the change was only a change in personnel. The NSA-NIST MOU had established the NSA Deputy Director for Information Security as the point of contact for the TWG, but SIGINT members had been filling the position. In September 1997 the IAD technical director, Brian Snow, became co-chair of the TWG. That signaled a change in approach. SIGINT's focus is on accessing communications, while IAD's interest is on securing them. The two sides of NSA had somewhat divergent views on whether communications security should be widely available for the private sector.

After Clipper, NIST sought to assert its role in securing non–national security systems. In 1997, NIST put out a call for a competition to replace the Data Encryption Standard (DES). In sharp contrast to the 1970s effort in choosing DES, NIST wanted the Advanced Encryption Standard (AES) competition to be a very public process. To NIST, this meant public inclusion from the beginning, including even in developing the requirements for the new standard.[65]

With Snow as TWG co-chair, the working group supported NIST's efforts to develop a strong, new encryption algorithm. NIST opened the AES competition to non-Americans, and meetings on AES candidates were public. Indeed, to encourage international participation, one of the evaluation meetings was held in Rome. Now NIST's expertise in cryptography was limited. As the Computer Security Act had provided, the standards agency had to rely on "the technical advice and assistance . . . of the National Security Agency" as needed.[66] But while NSA conducted tests on the security and speed of the AES submissions, NIST ran the show.[67]

The five algorithms that the private-sector cryptographers agreed were the strongest (there was a possible sixth contender) were exactly the five finalists selected by NIST from the original fifteen candidates. The winning candidate, Rijndael, had been designed by two Belgian researchers. This was quite remarkable. In contrast to the relatively secret proceedings around choosing DES, the competition for choosing AES was quite open—and ended up with a European-designed algorithm. Fears that the NSA was seeking to exercise tight control over private-sector cryptography began to ebb.

The November 2001 approval by the Department of Commerce of Rijndael as the Advanced Encryption Standard was particularly striking in that it occurred two months after the terrorist attacks of September 11, 2001. Even while aspects of the Foreign Intelligence Surveillance Act and other surveillance laws were being modified, no

[65] Announcing Development of a Federal Information Processing Standard for Advanced Encryption Standard, 62 Fed. Reg. 93 (Jan. 2, 1997).
[66] Computer Security Act, Pub. L. No. 100-235, § 2(b)(1) (1988) (repealed 2002).
[67] NSA discussions on how to position the agency regarding the AES competition ranged widely. The main options under consideration included submitting a candidate algorithm, cryptanalyzing the submissions for NIST, doing both, or doing neither. NSA chose to offer NIST support by cryptanalyzing AES candidates for NIST and offering hardware simulations for the candidates, so that NIST could review performance. Communication between Brian Snow and the author (Dec. 27, 2012) (on file with author).

administration official spoke publicly against the loosening of cryptographic export regulations that had occurred a year earlier. Instead the approval of Rijndael as the Advanced Encryption Standard went forward as planned. The NSA was clearly on board with approval of AES as a Federal Information Processing Standard.

In June 2003, a striking development occurred: the NSA approved the use of AES as a "Type 1" algorithm,[68] permitting AES to be used to protect classified information as long as it was in an NSA-certified implementation. At one stroke NSA vastly increased the market for products running the algorithm. This would have the converse effect of ensuring AES's wider availability in non-classified settings. NSA's activities in ensuring private sector communications security did not stop there.

An encryption algorithm is only one part of securing a communication network. Also needed are algorithms for establishing keys, for ensuring authenticity of the communication, and for performing message-integrity checks. In 2005 NSA approved "Suite B," a set of algorithms that included AES, Elliptic-Curve Diffie Hellman, Elliptic-Curve Digital-Signature Algorithm, and Secure Hash Algorithm for securing a communications network. NSA was clear about the rationale: networks using the Suite B set of algorithms would enable "the U.S. Government to share intelligence information securely with State and local First Responders and provid[e] war fighters on the battlefield the capability to share time-sensitive information securely with non-traditional coalition partners."[69]

NSA's creation of Suite B was valuable for users outside of the national-security community as well. All the algorithms in Suite B were unclassified (all, in fact, were FIPS). This meant Suite B could be deployed in non–national security settings and could be used to secure non–national security communications networks as well. This would complicate law-enforcement interception. Yet the NSA went forward with the approval of Suite B.

The NSA's active support of widely available communications-security tools went further. One of the problems highlighted during the September 11 attacks had been the lack of interoperability between communications systems used by the police and the firemen at the burning buildings in Manhattan. It is not uncommon for three sets of first responders—police, fire, EMTs—to be on three different communications systems, none interoperable. It is also likely that the systems of first responders in one locale are not interoperable with those of the same services the next county over. We saw the problem on September 11, when the police and firemen could not communicate with one another

[68] COMM. ON NAT'L SEC. SYS., NAT'L SEC. AGENCY, POLICY NO. 15, FACT SHEET NO. 1, NATIONAL POLICY ON THE USE OF THE ADVANCED ENCRYPTION STANDARD (AES) TO PROTECT NATIONAL SECURITY SYSTEMS AND NATIONAL SECURITY INFORMATION (2003).

[69] *Suite B Cryptography*, NAT'L SEC. AGENCY/CENT. SEC. SERVICE'S INFO. ASSURANCE DIRECTORATE, http://www.nsa.gov/ia/programs/suiteb_cryptography/ (accessed by searching the archived copy of an older version of the website, available at: http://archive.today/mFaN).

at the World Trade Center; we saw the problem five years later, when the same situation repeated itself with first-responder and relief groups during Hurricane Katrina.[70]

The communications device of choice for first responders is land mobile radio (LMR), which functions even when other communications networks, such as cellular communications or wire lines, are down. LMR does not have the line-of-sight access requirements of satellite phones, which can be blocked by cloud cover, tall buildings, or mountains. Of course it is important that communications between first responders be secure. Suite B enables this, and thus enables secure LMR to be developed as a mass-market item. NSA embraced this approach.

In 2010, Richard George, Technical Director at NSA's Information Assurance Directorate explained, "We've got Type 1 Suite B product that we can use at the highest level of communications,"—meaning in communications with the president—"and we've got to have straight commercial Suite B systems that are available at the mall, at Radio Shack, for first responders."[71] Given who else might purchase such systems, one could imagine controversy about widespread availability. But NSA was behind the project. "Everyone buys into the concept," George said.[72]

NSA also plays a role in the Security Automation Protocol (SCAP) initiative. Under the Cyber Security Research and Development Act of 2002, NIST was to develop checklists providing configuration settings that would "harden" computer systems against attacks. This was to be done for hardware and software products used by the government. While such information existed, in 2002 it remained largely hidden through obscurity,[73] written on pieces of paper filed at different agencies. NIST's job was to regularize things. This meant developing a process for collecting and publishing the information—that is, standardizing it. The result is SCAP, a set of security checklists in a standardized format, thus enabling them to be run automatically. The checklists include configurations for operating systems (Microsoft, Apple, Linux, Solaris), firewalls, routers, switches, etc. SCAP is considered a real success in the government cybersecurity story; it is run by NIST in cooperation with the NSA and the Defense Information Systems Agency.

NSA's public acknowledgement of ECC security at the 1995 ANSI meeting was a brief comment, crucial but nonetheless quietly stated. Standards work also occurs in fora where the record of the discussion itself is more permanent. For example, the Internet Engineering Task Force (IETF), an international group that produces technical and engineering documents—protocol standards, best practices, and informational

[70] Henry S. Kenyon, *Modernization Closes the Interoperability Gap*, SIGNAL ONLINE (Aug. 2007), http://www.afcea.org/content/?q=node/1365.
[71] Communication between Richard George and the author (Feb. 26, 2010) (on file with author).
[72] *Id*.
[73] One often talks about "security through obscurity," security achieved through hiding the mechanism for performing security. The argument for doing so is that it prevents the bad guys from figuring out how to get around the security mechanisms. But because the security system is not open to public scrutiny, such an approach is not considered a good one. Here we had the opposite: lack of security due to obscurity of the security mechanisms. This was similarly a poor approach to take.

documentation—"to make the Internet work,"[74] holds its discussions online. The result is a searchable record of each aside, note, and comment. In recent years, NSA participants have actively engaged in IETF discussions.[75] This is yet another way that the NSA has been effectively sharing its knowledge of securing communications infrastructure with the private sector. The contribution to the IETF is notable since the NSA insights into securing communications protocols are part of the public record for anyone from China to Iran to Russia (and points in between) to read.

V. A PROBLEM NOT OF THE IAD'S MAKING

As we now know, the agency's motivation in working in public security standards was not always above board. On at least one occasion, its efforts resulted in the adoption of a corrupted cryptographic standard. I will briefly discuss this before moving on to discuss the rationale behind the simultaneous efforts by NSA to secure public-sector communications.

According to leaked NSA documents, "SIGINT Enabling Project actively engages the U.S. and foreign IT industries to covertly influence and/or overtly leverage their commercial products' designs. These design changes make the systems in question exploitable."[76] "Base resources in this project are used to . . . insert vulnerabilities into commercial encryption systems [and] . . . influence policies, standards, and specifications for commercial public key technologies."[77]

The algorithm in question is Elliptic Curve Digital Random Bit Generator (Dual EC-DRBG). This is an important algorithm, at least in part because it was used by RSA Security LLC as the default random bit generator in its product BSAFE, a cryptographic toolkit. Dual EC-DRBG uses elliptic curves to generate random bits, which are needed for various cryptographic applications, including key generation. The randomness of such bits is thus crucial, since if the key bits are predictable, then no matter how strong the cryptography is, it will fail to secure the system. Because truly random bits are difficult to generate, the usual method is to start with some genuinely random bits and then use a mathematical function to stretch these bits into a longer sequence of "pseudo random bits" (bits that behave randomly for all practical purposes). That is what Dual EC-DRBG was supposed to do.

But there were oddities about Dual EC-DRBG. It was much slower than alternatives, there was no explanation for the choice of two default parameters, and the random bit generator provided more bits than it seemed secure to do. Nonetheless NIST approved it

[74] H. Alvestrand, *A Mission Statement for the IETF*, Oct. 2004, http://www.ietf.org/rfc/rfc3935.txt.
[75] *See, e.g.*, *[Cfrg] Status of DragonFly*, https://www.ietf.org/mail-archive/web/cfrg/current/msg03258.html.
[76] *Computer Network Operations: SIGINT Enabling*, N.Y. TIMES, Sept. 5, 2013, http://www.nytimes.com/interactive/2013/09/05/us/documents-reveal-nsa-campaign-against-encryption.html.
[77] [SECRET].

as a recommended algorithm (this was after RSA had adopted the algorithm as its default standard). Shortly afterwards, two Microsoft researchers demonstrated that knowledge of the relationship between the two parameters would allow an attacker to predict future random bits.[78] Despite the concerns being raised, NIST did not rescind its approval of the standard. Neither did RSA Security LLC change the default status of the algorithm in its BSAFE toolkit.

This all changed when leaked records surfaced in September 2013 describing NSA's role in pushing a draft security standard into a 2006 NIST Special Publication as "a challenge in finesse."[79] Although the documents did not specify Dual EC-DRBG, there was little question about the issue. NIST responded by recommending against use of the algorithm and reopened comments for the document that had recommended it.[80] Similarly RSA Security LLC issued an advisory urging its customers to stop their use of Dual EC-DRBG.

From implementations of SSL/TLS that relied on Dual EC-DRBG to generate the "Client Cryptographer Nonce" at the beginning of an SSL connection, to systems that employed the BSAFE toolkit (and specifically Dual EC-DRBG for random bit generation), the compromised algorithm was in use for nearly a decade in many places and forms. This enabled NSA to read any traffic or storage that relied upon the system. So while IAD had been quietly working to secure private-sector telecommunications infrastructure, SIGINT had provided a backdoor to a wide variety of systems, a backdoor to which, it should be noted, only NSA had the key.[81]

The situation did not end there. In 2008, a draft was submitted to the IETF, "Extended Random,"[82] that described an enhancement to Dual EC-DRBG producing additional random bits. In fact, anyone who employed Extended Random made it vastly simpler for users with Dual EC-DRBG backdoor information to break messages encrypted with the algorithm.[83] An analysis showed Extended Random was most effective when Dual EC-

---

[78] *See* Dan Shumow & Niels Ferguson, *On the Possibility of a Back Door in the NIST SP800-90 Dual EC PRNG*, Crypto Rump Session (2005), http://rump2007.cr.yp.to/15-shumow.pdf.
[79] Perlroth et al., *supra* note 6.
[80] Information Technology Laboratory, National Institute of Standards and Technology, *Supplemental ITL Bulletin for September 2013: NIST Opens Draft Special Publication 800-90A, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, for Review and Comment*, Sept. 2013, http://csrc.nist.gov/publications/nistbul/itlbul2013_09_supplemental.pdf.
[81] Dual EC-DRBG comes with two parameters, the genesis of which was never publicly explained. Anyone who knows the arithmetic relationship between these parameters can decrypt encrypted messages quickly. While the NSA has never publicly disclosed that it knows this relationship, the fact that no explanation was ever given on the origin of the parameters gives strong evidence that this is indeed the case.
[82] E. RESCORLA AND M. SALTER, EXTENDED RANDOM VALUES FOR TLS, INTERNET ENGINEERING TASK FORCE (Oct. 31, 2008).
[83] Stephen Checkoway, Matthew Fredrikson, Ruben Niederhagen, Matthew Green, Tanja Lange, Thomas Ristenpart, Daniel J. Bernstein, Jake Maskiewicz, and Hovav Shacham,
On the Practical Exploitability of Dual EC in TLS Implementations (Apr. 7, 2014), *available at:* http://dualec.org/DualECTLS.pdf.

DRBG was used with a large key (length of 384 or 521 bits).[84] Thus this "enhancement" was the very opposite of protective.

Who foisted this cryptographic weakness off on the private sector? It appears that the main author of the IETF Internet draft was Margaret Salter. [85] At the time, Salter was Technical Director of IAD's Evaluation Group, the group responsible for cryptanalysis and security review of products used to protect classified government data. By putting forward this algorithm, IAD compromised itself and risked destroying the public trust it had gained through its work on AES, Suite B, etc.

VI. THE RATIONALE

It is one thing to go from the NSA of the 1950s— No Such Agency—to having a press office. It is quite another to provide technical communications security expertise in public. IAD's efforts to secure private-sector communications are clearly beneficial, but they are also potentially disruptive of the SIGINT mission and of the FBI's domestic investigations. What caused this extraordinary change?

Part was changing technical capabilities outside NSA: the private sector was developing cryptographic capabilities that matched NSA's own. Part was changing political realities quite unrelated to cryptography or the NSA mission: the end of the Cold War meant cutbacks in defense spending. Part was an acknowledgement of the political realities: the bills in Congress, the conclusions of the National Research Council report, the fact that the Internet was changing not only communications methods but also enabling new exploitation capabilities. Part was an acknowledgement that the private sector's security needs were increasingly similar to the government's. And part was an intent to subvert the effect of some of these changes through network exploitation efforts, efforts that vastly increased in scale post–September 11, 2001.

The 1970s development of cryptography in the private sector led NSA to see "that there was opportunity out there."[86] In fact, the DES effort provided a wake-up call to NSA. In the immediate postwar period, there had been no serious non-governmental challenger to NSA's expertise, and the agency had been accustomed to performing all the research and development work for the government's secure communications systems. This meant doing the design, development, and the engineering development model. Contractors were brought in at essentially the final stages, their role being to build the actual apparatus. But DES, a strong cryptosystem, had been created by a different three-letter

[84] Daniel Bernstein, Tanja Lange, & Ruben Niederhagen, *Dual EC DRBG*, *available at*: https://projectbullrun.org/dual-ec/ext-rand.html.
[85] The second author was Eric Rescorla, chair of the particular IETF working group. He has not explained his participation in this draft.
[86] Communication between Mike Jacobs, former head of IAD, and the author (Jan. 4, 2013) (on file with author).

entity, IBM—not NSA. The effort showed there was a potential alternative development model, one that very much worked to the agency's advantage.

Begun in 1984, the Commercial Comsec Endorsement Program (CCEP) set up a system in which private companies built communications security technologies with NSA vetting.[87] There was a multi-step process in which vendors first approached NSA with a proposal for a communications security device. Then, if the agency felt that the product was sound from a technical standpoint and that the proposed product filled a niche in a particular environment, NSA and the company would sign a Memorandum of Understanding and they would work together to bring the product to market.[88] The situation was risky for the companies, for they were the ones that bore the development costs, a point not lost on the NSA. But sometimes the gamble paid off quite well: STU-IIIs, the most popular version in the series of secure telephones developed by the government, was built by four manufacturers, AT&T, Motorola, Nortel (notably, a Canadian company), and RCA, under the CCEP.[89]

The User Partnership Program (UPP), started in the late 1990s, was a more sophisticated version of the CCEP. It used the efforts of the various defense agencies, saving the resources of the IAD in the process. Instead of a vendor approaching the NSA with a proposal for a COMSEC device, the vendor partners with a government department or agency and then submits the proposal of the COMSEC devise to IAD for its blessing. As with the CCEP, the risks of development are borne by the vendor. But, in an advantage to both the vendor and the NSA, the partnering with a potential government buyer early in the process leads to a greater likelihood that the developed product will actually be one sought by a DoD customer. The CCEP and UPP efforts had another decided advantage for NSA,[90] namely the agency got a head start on examining industry security products.

The end of the Cold War brought about a sharp decrease in military spending,[91] and its ending provided another impetus for NSA's turn to commercial systems. In 1994 Secretary of Defense William Perry directed DoD contractors to use COTS products unless the *only* alternative was a custom military design.[92] The 1996 Clinger-Cohen Act[93] required that information technology[94] use commercial technology where possible. The

[87] *See* DEPARTMENT OF DEFENSE, COMSEC SUPPLEMENT TO THE INDUSTRIAL SECURITY MANUAL FOR SAFEGUARDING CLASSIFIED INFORMATION 12 (1988).
[88] Ellen Messmer, *NSA Program Results in Secure Net Wares*, NETWORK WORLD (Sept. 10, 1990).
[89] *Id*.
[90] The same advantage occurred as a result of requiring export licenses for products containing cryptography; *see, e.g.*, Whitfield Diffie & Susan Landau, *The Export of Cryptography in the 20th Century and the 21st*, *in* THE HISTORY OF INFORMATION SECURITY: A COMPREHENSIVE HANDBOOK (Karl De Leeuw & Jan Bergstra eds., 2007).
[91] *See* OFFICE OF MGMT. AND BUDGET, OFFICE OF THE PRESIDENT, HISTORICAL TABLES: BUDGET OF THE U.S. GOVERNMENT (FISCAL YEAR 2011), Table 8.4.
[92] Ivan Eland, *Can the Pentagon be Run Like a Business?*, 18 ISSUES IN SCIENCE AND TECH. 78 (2002).
[93] 40 U.S.C. § 1401 et seq.
[94] This is "equipment or [an] interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching,

Federal Acquisition Regulations (FAR), part 12.101 stated that agencies "(a) conduct market research to determine whether commercial items or nondevelopmental items are available that could meet the agency's requirements; (b) acquire commercial items or nondevelopmental items when they are available to meet the needs of the agency; and (c) require prime contractors and subcontractors at all tiers to incorporate, to the maximum extent practicable, commercial items or nondevelopmental items as components of items supplied to the agency."

There was another aspect to this issue: the rapid pace of technological change. The pace was effectively putting NSA's customized solutions out of business, and the agency had to adapt to the new reality. The agency went public with its intent to embrace secure COTS products. In a 2002 keynote before Black Hat, a computer-security conference dominated by hackers, IAD Technical Director Richard George laid out the plan,

> NSA has a COTS strategy, which is: when COTS products exist with the needed capabilities, we will encourage their use whenever and wherever appropriate . . . That's where we need to be careful. In my view, that's where the government, NSA in particular, can be most helpful: working with the private sector to ensure that U.S. commercial products provide the security needed by our critical infrastructure and our citizens as well. In fact, we have a responsibility to do everything we can to work with U.S. industry to make U.S. products the best in the world; to make U.S. security products the products of choice world-wide. That brings us to this point of the discussion. If we—government and critical infrastructures—are going to COTS products, where is IA going: Does that mean we're giving up on assurance? Absolutely not. There has been a migration in DoD thinking from a "risk avoidance" model to a "risk management" model. This is more a change in advertising than in reality; we know we always had risks, we're just sharing more risk information with the customer so that we can work together to decide which risks are smart to take, and what steps we can take—policies, procedures, etc.—to lessen these risks.[95]

A recent IAD effort, Commercial Solutions for Classified (CSfC), is an example of leveraging work from the commercial sector. CSfC "layers" products from government efforts with those from private industry to develop communication tools with high security.[96] The government products have high assurance, high lifecycle costs, and slow development processes; the commercial products have varying levels of assurance, lower lifecycle costs, and faster development processes. Security comes partially through that provided by the individual products and partially through the independence provided by their differing approaches. For example, in combining a hardware encryptor from Vendor A with a software one from Vendor B, each encryptor runs a different protocol, on a

---

interchange, transmission, or reception of data or information by the executive agency." 40 U.S.C. § 1401(3) (now 40 U.S.C. 11101 (6)).

[95] Richard George, Technical Director, Security Evaluations Group, National Security Agency, Keynote Address at Black Hat Briefings 2002 (Jul. 31, 2002).

[96] Fred Roeper, Technical Director, National Security Agency, & Neal Ziring, Technical Director, National Security Agency, Address at RSA Conference 2012 (Mar. 2, 2012).

different platform, and is built on a different codebase. This provides more security than using either system on its own. To participate in the CSfC program, commercial products must satisfy certain NSA security requirements.[97]

The fundamental idea of combining different components to increase security works for clients other than just the government. Because the parts can be from commercial systems, such a technique can be used to provide security for any user, not just government ones.[98] Notably, and in line with other efforts to improve private-sector communications security, IAD has been discussing this methodology in public, and not confining knowledge of it simply to the defense community.

COTS formed the backbone of the Cryptographic Modernization Program (CMP) a multi-billion-dollar NSA program to modernize secure DoD communications systems. Its purpose was to unify and simplify: move communications security from stovepiped solutions into commercial, network-centric solutions. Begun in 1999, CMP was a multi-decade long effort, still in progress today.

This shift would provide new challenges. Even when the agency was the sole developer of secure equipment, NSA had always had trouble ensuring that communications security was observed in the field. As an NSA history of the Vietnam War reported, "No matter how dramatic the evidence of threat, if we simply go out and say, 'Stop using your black telephone,' it's likely to be effective for about two weeks."[99] Now DoD would be using COTS equipment much of the time. One might think that would undermine NSA's ability to ensure that communications in theater were well secured. In fact, the old system of government proprietary algorithms made information sharing difficult and often prevented interoperability[100]—and thus security was frequently turned off. The new systems of COTS equipment could fix some of these difficulties. But unless the new systems have the critical feature of automatically going secure, the problem of communications traveling over unprotected channels will remain. However, increasing speed and decreasing cost makes all sorts of automatic security possible, as Google discovered when, in 2010, the company made https the standard protocol for transmitting Gmail.[101]

Changing defense economics was one issue, but changing military alliances raised a different one. Long-term military alliances such as NATO develop secure communication systems that interoperate with member states' militaries. But the 1990s and 2000s saw the

---

[97] *Commercial Solutions for Classified Program*, NAT'L SEC. AGENCY/CENT. SEC. SERVICE'S INFO. ASSURANCE DIRECTORATE, http://www.nsa.gov/ia/programs/csfc_program/.

[98] Roeper & Ziring, *supra* note 92.

[99] DAVID BOAK, A HISTORY OF U.S. COMMUNICATIONS SECURITY (VOLUME II): THE DAVID G. BOAK LECTURES 10 (1973).

[100] *See* Kenyon, *supra* note 70.

[101] The http protocol transmits communications in the clear, so that anyone eavesdropping on the communication, say by a man-in-the-middle attack, by listening in on a compromised switch or router, etc., can see the communication. The https protocol provides "end-to-end" security for the communication. In the case of Gmail, this means that the mail is encrypted from the user to the Gmail server.

United States in a new type of military operation: short-term alliances with partners whom the U.S. neither trusted nor necessarily sought to have long-term military partnerships with. The 1991 Gulf War and the 1998–1999 Kosovo War are examples of these. The U.S. needed secure communication systems that could be stood up quickly, but that would not reveal the technologies behind secure government communication systems. The fact that the private sector was now developing secure communication systems provided a way out of the problem.

Thus in 1999 the NSA launched the Cryptographic Interoperability Strategy, "developed to find ways to increase assured rapid sharing of information both within the U.S. and between the U.S. and her partners through the use of a common suite of public standards, protocols, algorithms and modes referred to as the 'Secure Sharing Suite' or S.3."[102] One such use was enabling "war fighters to securely share information on the battlefield with non-traditional coalition partners."[103]

The government was not the only one in need of high-quality communications security. Industry is now deeply reliant on the Internet—for use in communicating with customers and business partners, for internal communications, and for enabling outsourcing[104]—created a set of security needs for industry that was different in kind.

While economic espionage has been a threat to U.S. industry for several decades, and was serious enough to warrant the Economic Espionage Act, the fact is that accomplishing such theft typically took years of work. The Internet changed the playing field in two fundamental ways. Proprietary information—business plans, research and development work, trade secrets—was no longer in locked file cabinets but in locked computer files. And the locks were often easy to get around. To make matters worse, the file cabinets were not in an office or factory floor in Denver or Des Moines, but in a computer accessible via the network.

During the Cold War, much industrial spying was done through "scientific" exchanges between the West and the U.S.S.R. Collaborative working groups in agriculture, civil aviation, nuclear energy, oceanography, computers and the environment were supported by Soviet case officers.[105]A well-known case within industry is that of Fairchild Semiconductor. Between 1977 and 1986, the company had up to 160 thousand pages'

---

[102] *Suite B Cryptography*, NAT'L SEC. AGENCY/CENT. SEC. SERVICE'S INFO. ASSURANCE DIRECTORATE, http://www.nsa.gov/ia/programs/suiteb_cryptography/ (accessed by searching the archived copy of an older version of the website, available at: http://archive.today/mFaN).

[103] *Id.*

[104] During the 1990s and increasingly so in the 2000s, companies began outsourcing functions previously done in-house. This ranged from such obvious functions as travel agencies and managing employee health care, to outsourcing manufacture of core company products. *See, e.g.*, SUSAN LANDAU, SURVEILLANCE OR SECURITY?: THE RISKS POSED BY NEW WIRETAPPING TECHNOLOGIES 154–57 (2011). Outsourcing presents a number of security challenges, for it changes the boundaries of the company. One obvious aspect is that communications between the company and its outsourcing partner must be secured; that is achieved through encryption.

[105] Matthew French, *Tech Sabotage During the Cold War*, FED. COMPUTER WEEK (Apr. 26, 2004), http://fcw.com/articles/2004/04/26/tech-sabotage-during-the-cold-war.aspx.

worth of proprietary data stolen and shared with the Japanese consulate in San Francisco. Fairchild needed the U.S. government to defend itself against a 1986 attempted takeover by Fujitsu.[106] Now a major theft of intellectual property can be accomplished in a matter of months. An industry spy first develops a computer payload that burrows deeply within the target's system, and then, at a time of the spy's choosing, leaks out potentially huge amounts of proprietary data. Arranging for Russian—or Chinese, Iranian, or German—hackers to intrude into the computer systems of U.S. corporations to steal information takes much less time to organize than the equivalent in the pre-Internet day. Such an exploitation can yield extensive results. The Internet's arrival changed what had been a relatively low trickle of economic espionage to an unmanageable flood.

For a time, cyber exploitations—computer intrusions for stealing information—of U.S. industry and government sites were occurring without public acknowledgement. This changed in 2005 with *Time* magazine's reporting that hackers, purportedly from China, had exfiltrated a number of classified files from four U.S. military sites in 2004.[107] The files included Army helicopter and flight-planning software. *Time* described thefts from various defense contractors and NASA as well.[108] These news stories opened the floodgates. Reports began appearing from every sphere of U.S. industry, including consumer-oriented firms such as Disney, General Electric, and Sony, high-technology companies such as Google, Symantec, and Yahoo, energy companies including BP, Conoco, and Exxon Mobil, and defense contractors such as Lockheed Martin and Northrop Grumman.[109] The theft was of software, products in development, trade secrets, and business plans, the intellectual property that is the very lifeblood of modern, technologically oriented firms. The attackers vary, sometimes from Russia (whose focus is heavily on energy-related industries), sometimes from China, sometimes from other nations, including U.S. military and diplomatic allies. By 2011, Deputy Secretary of Defense William Lynn III described cyber exploitation as the "most significant" cyber-threat facing the U.S. over the long term.[110] For a long time the U.S. government was

---

[106] INTERAGENCY OPSEC SUPPORT STAFF, INTELLIGENCE THREAT HANDBOOK 39–40 (2004), http://www.fas.org/irp/threat/handbook/economic.pdf.

[107] *See* Nathan Thornburgh, *Inside the Chinese Hack Attack,* TIME (Aug. 25, 2005), http://www.time.com/time/nation/article/0,8599,1098371,00.html.

[108] Nathan Thornburgh, *The Invasion of the Chinese Cyberspies*, TIME, Aug. 29, 2005, http://www.time.com/time/magazine/article/0,9171,1098961-1,00.html.

[109] Northrop Grumman and Yahoo are listed as targets in Ariana Eunjung Cha & Ellen Nakashima, *Google China Cyberattack Part of Vast Espionage Campaign, Experts Say*, WASH. POST (Jan. 14, 2010), http://www.washingtonpost.com/wp-dyn/content/article/2010/01/13/AR2010011300359.html. Information that Disney, General Electric, and Sony were affected appeared in Fahmida Y. Rashid, *HBGary E-mail Says DuPont Hit by China's Operation Aurora Attack*, EWEEK (Mar. 3, 2011), http://www.eweek.com/c/a/Security/HBGary-Emails-Say-DuPont-Hit-by-Chinas-Operation-Aurora-Attack-306724/. That BP, Conoco Phillips, and Exxon Mobil were attacked is from Michael Joseph Gross, *Enter the Cyber-dragon*, VANITY FAIR, Sept. 2011, http://www.vanityfair.com/culture/features/2011/09/chinese-hacking-201109. The attacks on Lockheed Martin were reported in Mathew J. Schwartz, *Lockheed Martin Suffers Massive Cyberattack*, INFO. WEEK (May 30, 2011), http://www.informationweek.com/government/security/lockheed-martin-suffers-massive-cyberatt/229700151.

[110] William J. Lynn III, *Defending a New Domain: The Pentagon's Cyberstrategy*, FOREIGN AFF., Sept./Oct. 2010, http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain.

cagey about what it knew about the scope and scale of this industrial espionage, but the publication of a highly detailed report on the scope and scale of the Chinese efforts by the security firm Mandiant[111] has changed both the government's willingness to respond publicly as well as industry's willingness to admit to having been exploited.[112] In any case, the changing communication security needs of U.S. industry thus provide yet another reason for the NSA's increasing efforts to provide security solutions for private-sector communications infrastructure.

From the 1950s to the early 1970s, the NSA had the field of COMSEC to itself. That was then; this is now. As Mike Jacobs, former IAD director put it, "We owned the space; we don't own it anymore."[113] The world is different, and for the nation's security, IAD's role needed to be different. This was recognized by the directorate, which acted in a far-sighted manner by expanding its efforts in a purely voluntary, non-regulatory way.

It did not escape NSA's notice that putting high quality communication-security tools in the hands of non-traditional coalition partners meant that those same tools would be accessible to other users. It similarly did not escape the agency's notice that secure communications equipment available for sale in Radio Shack would be available to police and criminals alike.

If IAD acted in one way, the documents leaked by Snowden show SIGINT was behaving in quite another. NSA's Office of Tailored Access Operations (TAO) had developed a remarkable toolkit of Computer Network Exploitation (CNE) techniques in the decade after September 11, 2001.[114] TAO, which was started in 1997, but which expanded greatly in recent years,[115] appears to have the capability to stymie the security provided by firewalls, firmware, operating systems, etc. of virtually all major manufacturers.[116] The value of these tools comes from the fact that data in transit is increasingly encrypted. By thwarting firewalls, firmware, etc., the NSA is able to exploit end-user devices, allowing SIGINT to collect data before it is encrypted—or after it has been received and decrypted. The security protections provided by IAD to the public could, in many cases, be undermined by TAO tools.

---

[111] *See generally* MANDIANT, *APT1: Exposing One of China's Cyber Espionage Units* (2013), *available at* http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf. *See also* David E. Sanger, David Barboza & Nicole Perlroth, *Chinese Army Unit is Seen as Tied to Hacking Against U.S.*, N.Y. TIMES, Feb. 18, 2013, at A1.

[112] *Admitting to Security Breaches*, N.Y. TIMES, Feb. 20, 2013; Nicole Perlroth & Nick Bilton, *Facebook Says Hackers Breached Its Computers*, N.Y. TIMES, Feb. 15, 2013.

[113] Interview with Mike Jacobs, Former Head, Information Assurance Directorate, National Security Agency (Feb. 4, 2013) (on file with author).

[114] *See Inside TAO: Documents Reveal Top NSA Hacking Unit*, DER SPIEGEL (Dec. 29, 2013), http://www.spiegel.de/international/world/the-nsa-uses-powerful-toolbox-in-effort-to-spy-on-global-networks-a-940969.html.

[115] *Id.*

[116] *See* Jacob Appelbaum, Judith Horchert & Christian Stocker, *Shopping for Spy Gear: Catalog Advertises NSA Toolbox*, DER SPIEGEL, Dec. 29, 2013, http://www.spiegel.de/international/world/catalog-reveals-nsa-has-back-doors-for-numerous-devices-a-940994.html.

It is tempting to ask whether IAD's public security efforts were merely an elaborate decoy to hide SIGINT's extensive surveillance exploits. This seems unlikely. Clearly NSA senior leadership knew that NSA was capable of countering the security technologies being provided by IAD, but that somewhat misses the point. It does not actually matter whether IAD leadership knew the particulars of TAO capabilities. For the critical point is that the use of TAO tools appears to have been limited to highly targeted situations, while the IAD tools provided to the private sector could be deployed broadly.

One can argue whether NSA surveillance was excessive, but that is not the subject of this paper. While collection could sometimes be quite vast (one example of this is domestic metadata), it appears that the use of TAO tools for acquisition was significantly more limited. Nothing in the leaked documents has so far shown otherwise. What this means is that the capabilities IAD was providing for security could indeed be effective despite the NSA's remarkable capabilities when targeting specific individuals. Thus it really is the case that IAD provided capabilities for securing for private-sector telecommunications infrastructure. This remains true even though IAD also participated in the "Extended Random" effort.

VII. WHERE DO WE GO FROM HERE?

It is impossible to discuss the communications security side of NSA without acknowledging the Snowden leaks, which exposed a vast system of collection of content by the NSA's SIGINT: bulk collection of domestic metadata,[117] targeting of Internet communications and stored metadata of non-U.S. persons,[118] highly targeted surveillance against close U.S. allies,[119] tapping of U.S. Internet company inter-data center communications,[120] etc. From the point of view of the COMSEC organization, however, two particular revelations stand out: the TAO program and the "finessing" of a cryptographic standard into which NSA had placed an apparent backdoor.[121] These two efforts are, however, quite different. Even if the scale of the TAO program is somewhat overwhelming, the program itself was within the normal parameters of signals intelligence work. Subverting the cryptographic standards process so that a flawed algorithm, Dual EC-DRBG, was recommended for use by NIST was a different matter entirely. This very badly damaged trust in NIST, which since the AES effort had developed a reputation as an honest broker in the cryptographic standards world.

---

[117] Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, GUARDIAN, June 5, 2013, http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.
[118] Glenn Greenwald, *NSA Prism Program Taps in to User Data of Apple, Google and Others*, GUARDIAN, June 6, 2013, http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.
[119] *Embassy Espionage: The NSA's Secret Spy Hub in Berlin*, DER SPIEGEL, Oct. 27, 2013, http://www.spiegel.de/international/germany/cover-story-how-nsa-spied-on-merkel-cell-phone-from-berlin-embassy-a-930205.html.
[120] Gellman & Soltani, *supra* note 2.
[121] Perlroth, Larson & Shane, *supra* note 6.

This said, the damage caused by NSA SIGINT efforts to communications security is not the subject of this paper. Rather I return to NSA efforts over the last two decades to secure domestic communications infrastructure. The president's NSA Review Committee[122] has made numerous recommendations in response to information resulting from the Snowden leaks. The one that concerns us here is that IAD separate from NSA and become its own agency reporting to the cyber policy effort within the office of the secretary of defense.[123]

The review committee's rationale had a number of reasons, most prominently that "the SIGINT function and the information assurance function conflict more fundamentally than before."[124] The experience with Dual EC-DRBG shows the truth of that statement. The review committee said that IAD's need to collaborate with the civilian sector, including industry and academia, argued for the need to place the organization outside the signals-intelligence agency. Yet that change seems unlikely to occur. As the review committee report noted, there is great value in sharing technical information between the SIGINT and COMSEC sides of NSA. Indeed, individuals at the agency benefit from the ability to go back and forth between the two halves; the committee report observed, "Such collaboration could and must occur even if IAD is organizationally separate."[125] Even if IAD were to be spun off from the NSA, NSA would need to retain some information-assurance capability. Given that, and the fact that the U.S. government has little appetite for duplicative efforts from competing agencies, it seems quite unlikely that this recommendation will be acted upon.

Nonetheless, it is certainly the case that IAD's initiative in providing the private sector with security solutions for communications infrastructure not only makes sense from a national-security perspective; it is quite appropriate given the critical importance of private communications infrastructure to U.S. national security. The fact that IAD began doing so beginning in at least 1995 was prescient, and the real question is how this effort should proceed. The effort has been both useful and admirable, but doing such security work for the private sector is not directly within NSA's mission. The question is where to go from here. While NSA's expertise in finding vulnerabilities within communications systems is unmatched within the U.S. government, from a business and geopolitical standpoint, the agency is the wrong institution to be providing private-sector telecommunications providers with security expertise. This was true even before the Snowden leaks created tremendous domestic and international distrust of the U.S. national security agency.

Telecommunications is not only run by the private sector, it is largely an international business. Though IAD's intentions appear to have been pure, it was already impossible

[122] *See* REVIEW GROUP ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGIES, LIBERTY AND SECURITY IN A CHANGING WORLD: REPORT AND RECOMMENDATIONS OF THE PRESIDENT'S REVIEW GROUP ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGIES (2013).
[123] *See id.* at 34.
[124] *Id.* at 185.
[125] *Id.* at 192–93.

prior to Snowden for the NSA to take the lead in providing security solutions for communications infrastructure. In light of the information we now know, the question is whether any agency of the U.S. government can do so, not whether IAD can. If the U.S. government is to be successful in providing technologies and technical advice for securing private-sector communications infrastructure, this must be done instead by an entity[126] more in synch with the needs of the private sector and the international community.[127]

Such realities should not diminish the importance of nearly two decades of efforts by IAD to secure private-sector communications infrastructure. These efforts had various important impacts, such as enabling and increasing the deployment of the Advanced Encrypted Standard. This work was accomplished during a time of great societal and political change. There was massive disruption in telecommunications and communications security and major shifts in international power. NSA provided important initial steps for securing communications infrastructure during this time of upheaval. Now we must determine how best to move forward.

[126] The natural agency within the U.S. government to do so is NIST. However, because NIST had recommended the use of Dual EC-DRBG for random bit generation—and did not reexamine the security concerns in 2007 when questions were raised about the algorithm's choice of parameters—the agency has also been tainted by the recent leaks regarding NSA surveillance efforts. NIST has begun a formal review of its standards process, but it will have to work to reestablish the international trust and credibility it had previously enjoyed. I explore the options in a forthcoming paper.

[127] An early version of this, "A Proposal for a Joint NIST–NSA Effort to Secure Telecommunications Infrastructure," was submitted to the NIST Advisory Board in January 2013.