ARTICLE

DUELING OVER DUAL_EC_DRBG: THE CONSEQUENCES OF CORRUPTING A CRYPTOGRAPHIC STANDARDIZATION PROCESS

Nadiya Kostyuk and Susan Landau[*]

ABSTRACT

In recent decades, the U.S. National Institute of Standards and Technology (NIST), which develops cryptographic standards for non-national security agencies of the U.S. government, has emerged as the de facto international source for cryptographic standards. But in 2013, Edward Snowden disclosed that the National Security Agency had subverted the integrity of a NIST cryptographic standard—the Dual_EC_DRBG—enabling easy decryption of supposedly secured communications. This discovery reinforced the desire of some public and private entities to develop their own cryptographic standards instead of relying on a U.S. government process. Yet, a decade later, no credible alternative to NIST has emerged. NIST remains the only viable candidate for effectively developing internationally trusted cryptography standards.

Cryptographic algorithms are essential to security yet are hard to understand and evaluate. These technologies provide crucial security for communications protocols. Yet the protocols transit international borders; they are used by countries that do not necessarily trust each other. In

[*] Nadiya Kostyuk, Assistant Professor at the School of Public Policy and the School of Cybersecurity and Privacy at Georgia Institute of Technology, and Susan Landau, Bridge Professor in Cyber Security and Policy, Fletcher School of Law & Diplomacy and School of Engineering, Department of Computer Science, Tufts University. The work was done, in part, while Kostyuk was a Cybersecurity Policy Predoctoral Research Fellow, Fletcher School of Law and Diplomacy, Tufts University. This research was supported in part by funding from the William and Flora Hewlett Foundation under grant 2018-7277.

We greatly appreciate the help provided by Jon Lindsay, Michael Poznansky, and other members of the Digital Issues Discussion Group, as well as from Steven M. Bellovin, Dan Bernstein, Lily Chen, Donna Dodson, Bart Jacobs, John Kelsey, Brian LaMacchia, Tanja Lange, Adam Langley, Steve Lipner, Kerry McKay, Abraham Newman, Kenny Paterson, Bart Preneel, Steve Purser, Andrew Regenscheid, and additional researchers who preferred to stay anonymous.

particular, these nations do not necessarily trust the developer of the cryptographic standard.

Seeking to understand how NIST, a U.S. government agency, was able to remain a purveyor of cryptographic algorithms despite the Dual_EC_DRBG problem, we examine the Dual_EC_DRBG situation, NIST's response, and why a non-regulatory, non-national security U.S. agency remains a successful international supplier of strong cryptographic solutions.

CONTENTS

INTRODUCTION

The Internet presents a serious conundrum. Though well known to have security problems, the network is globally relied upon for commerce and used to control many critical systems and infrastructure. This inconsistency is partially explained by the fact that when someone says, "The Internet is insecure," they are often not referring to the communications network, but rather the applications that run on it. But it is also true that a

network itself can be insecure and nonetheless be widely used—because the network provides value and risk can be managed.

The Internet's communications protocols—TCP/IP—do not authenticate communication senders; this allows various attacks, including Distributed Denial of Service (DDoS), and simplifies attacker intrusions into endpoint networks. The decentralized nature of Internet routing—routers on the network share routing information with their neighbors—allows packets to be routed incorrectly,[1] sometimes leading to eavesdropping on communications, theft,[2] and even shutting down important and well-known websites due to traffic diversion.[3]

A solution to many of these problems exists: cryptography. The technology, which can provide confidentiality (ensuring no one but the intended recipients can read a message), integrity (ensuring that the communication has not been altered), and authenticity (proof that the message came from an authorized source), is essential to providing security and privacy to communications protocols (e.g., https).

Cryptography presents a peculiar problem to communications security. Cryptographic algorithms have been used to provide confidentiality, integrity, and authentication to many Internet communications protocols. These include, for example, the cipher suites[4] in TLS,[5] which is the protocol

---

[1] This is known as Border Gateway Protocol (BGP) hijacking.

[2] If a router directs a user to the incorrect site purporting to be the real one, the user may be tricked into authenticating herself, thereby giving away her user credentials.

[3] Declan McCullagh, *How Pakistan Knocked YouTube Offline (and How to Make Sure it Never Happens Again)*, CNET (Feb. 25, 2008), https://www.cnet.com/news/how-pakistan-knocked-youtube-offline-and-how-to-make-sure-it-never-happens-again [https://perma.cc/PKL4-DYPV].

[4] In TLS 1.3, these include Diffie-Hellman for key exchange, Advanced Encryption Standard in two key lengths (128 and 256 bits), ChaCha20 (a stream cipher) and related authenticator Poly1305, and the SHA256 cryptographic hash algorithm. Eric Rescorla, *Request for Comments No. 8446: The Transport Layer Security (TLS) Protocol Version 1.3*, INTERNET ENG'G TASK FORCE (Aug. 2018), https://datatracker.ietf.org/doc/html/rfc8446 [https://perma.cc/4HY7-78GN]; Y. Nir & A. Langley, *Request for Comments No. 8349: ChaCha20 and Poly1305 for IETF Protocols*, INTERNET ENG'G TASK FORCE (June 2018), https://datatracker.ietf.org/doc/html/rfc8439 [https://perma.cc/YFX2-CLAD]; A. Langley, M. Hamburg & S. Turner, *Request for Comments No. 7748: Elliptic Curves for Security*, INTERNET ENG'G TASK FORCE (Jan. 2016), https://datatracker.ietf.org/doc/html/rfc7748 [https://perma.cc/E4QL-TS5W].

[5] From the point of view of security, TLS 1.3 is a vast improvement over TLS 1.2. It introduces forward secrecy, in which new encryption keys are used for each communication session, sharply reduces the number of choices of implementations (which public-key algorithm with which private-key algorithm), thus reducing complexity (the bane of

that provides end-to-end security for web browsing, email, and other Internet applications. For a protocol such as TLS to transit international borders and securely transmit IP-based communications, there must be international acceptance and use of the cryptography employed within the protocols.[6] Protocols transit international borders of nations that do not necessarily trust each other—and, in particular, do not necessarily trust the developer of the cryptographic standard. In spite of this lack of trust, the use of these cryptographic standards has prevailed—an impressive success.

There have been occasional breaks in protocols and more frequent ones in the implementation of communications protocols. But breaks of approved cryptographic standards are quite uncommon, in large part due to public vetting of the proposed standards prior to adoption. One situation where such a break occurred deserves particular attention. In September 2013, *The New York Times, ProPublica,* and *The Guardian* reported that the NSA "[had] been deliberately weakening international encryption

---

security), eliminates problematic ciphers from being considered, speeds up and secures the "handshake" between two systems in which they negotiate a key, and allows encryption in "resumed" messages between two entities. *See* Nick Sullivan, *A Detailed Look at RFC 8446 (a.k.a. TLS 1.3)*, CLOUDFLARE BLOG (Aug. 10, 2018), https://blog.cloudflare.com/rfc-8446-aka-tls-1-3 [https://perma.cc/3EFQ-A7CA]; Rescorla, *supra* note 4. The former provides a simplified explanation, and the latter gives more technical details.

[6] In fact, in 2019 Russia explored banning the use of TLS 1.3, apparently because the protocol could be used to hide the name of a destination website. This would thwart government censorship and surveillance efforts. *See* Федеральный Закон о внесении изменений в статьи 2 и 10 Федерального закона «Об информации, информационных технологиях и о защите информации» [Federal Law on Amendments to Articles 2 and 10 of the Federal Law "About Information Technologies, and Protection of Information"], July 27, 2006, https://www.documentcloud.org/documents/7215232-Proposed-Russia-law-to-ban-secure-encryption.html [https://perma.cc/R4UG-6R5X]; Пояснительная Записка к проекту Федерального закона «О внесении изменений в статьи 2 и 10 Федерального закона «Об информации, информационных технологиях и о защите информации» [Explanatory Note to the Draft Federal Law "About Information Technologies, and Protection of Information"], Dec. 4, 2019, https://www.documentcloud.org/documents/7215233-149-%D0%9F%D0%97.html [https://perma.cc/F5QM-GJNG]. These laws had not yet entered into force when this article was written.

standards."[7] The *Times* pointed to an algorithm, Dual_EC_DRBG,[8] about which cryptographers had previously expressed doubts regarding its security. The algorithm, which supplied "random bits" for determining an encryption key, apparently had a cryptographic "backdoor."[9] Such a backdoor functions much like a key under a doormat, providing a way for those who know it to bypass the encryption and access the encrypted content.

In this case, the key under the doormat was the relationship between two parameters of the curve. Each elliptic-curve cryptosystem has two parameters, P and Q. If the curves are secure curves suitable for use in cryptography,[10] then finding a mathematical relationship between P and Q is computationally infeasible. But there was strong reason to believe that the NSA knew the mathematical relationship between the two parameters in

---

[7] Nicole Perlroth, Jeff Larson & Scott Shane, *N.S.A. Able to Foil Basic Safeguards of Privacy on Web*, N.Y. TIMES (Sept. 5, 2013), https:/www.nytimes.com/2013/09/06/us/nsa-foils-much-internet encryption.html [https://perma.cc/29GU-C6BQ]. *See also* Jeff Larson, *Revealed: The NSA's Secret Campaign to Crack, Undermine Internet Security*, PROPUBLICA (Sept. 5, 2013), https://www.propublica.org/article/the-nsas-secret-campaign-to-crack-undermine-internet-encryption [https://perma.cc/K87Z-24JE]; James Ball, Julian Borger & Glenn Greenwald, *Revealed: how US and UK spy agencies defeat internet privacy and security*, GUARDIAN (Sept. 6, 2013), https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security [https://perma.cc/9ZVH-CP4D].

[8] The original news article by Perlroth, et al., *supra* note 7, did not explicitly name the standard but made clear which it was. The accompanying NSA documents included such statements as "influence policies, standards and specification for commercial public key technologies" and "shape the worldwide commercial cryptography marketplace to make it more tractable to advanced cryptanalytic capabilities being developed by NSA/CSS." *See Secret Documents Reveal N.S.A. Campaign Against Encryption*, N.Y. TIMES (Sept. 5, 2013), https://archive.nytimes.com/www.nytimes.com/interactive/2013/09/05/us/documents-reveal-nsa-campaign-against-encryption.html [https://perma.cc/M5ND-RACD] [hereinafter *Secret Documents*]; Larson, *supra* note 7; Ball, Borger & Greenwald, *supra* note 7. Dual_EC_DRBG was identified several days later. *See* Nicole Perlroth, *Government Announces Steps to Restore Confidence in Encryption Standards*, N.Y. TIMES (Sept. 10, 2013).

[9] Perlroth, et al., *supra* note 7.

[10] Essentially this means avoiding "supersingular" curves and "prime-field anomalous elliptic" curves. *See* Alfred J. Menezes, Tatsuaki Okamoto & Scott A. Vanstone, *Reducing Elliptic Curve Logarithms to Logarithms in a Finite Field*, 39 IEEE TRANSACTIONS ON INFORMATION THEORY 1639, 1639 (1993); Takakazu Satoh & Kiyomichi Araki, *Fermat Quotients and the Polynomial Time Discrete Log Algorithm for Anomalous Elliptic Curves*, 47 COMMENTARII MATHEMATICI UNIVERSITATIS SANCTI PAULI 81, 81–82 (1998); I. A. Semaev, *Evaluation of Discrete Logarithms in a Group of p-Torsion Points of an Elliptic Curve in Characteristic p*, 67 MATHEMATICS COMPUTATION 353, 353–55 (1998); N. P. Smart, *The Discrete Logarithm Problem on Elliptic Curves of Trace One*, 12 J. CRYPTOLOGY 193, 193 (1999). These characteristics of elliptic curves are easy to test for and thus do not present problems in practice. Neal Koblitz & Alfred Menezes, *A Riddle Wrapped in an Enigma*, 14 IEEE SEC. & PRIV. 34, 37–38 (2016).

Dual_EC_DRBG.[11] Knowing this would provide the agency with a backdoor that allowed it to quickly decrypt communications ostensibly secured through Dual_EC_DRBG.[12] In addition, there appeared to be statistical bias in Dual_EC_DRBG's output,[13] a major flaw in any random-bit generator. This bias simplified the use of the backdoor for anyone with knowledge of the mathematical relationship between P and Q.

Even worse, the system was an approved cryptographic standard. When Dual_EC_DRBG had initially been proposed as a standard, a number of cryptographers raised concerns about the potential of a cryptographic backdoor.[14] Despite the cryptographers' misgivings, the National Institute of Standards and Technology (NIST) approved[15] Dual_EC_DRBG as a Federal Information Processing Standard (FIPS),[16] a standard for non-national

---

[11] In 2007, which was after the standard's approval, Dan Shumow and Niels Ferguson raised the possibility of a backdoor in the algorithm. Dan Shumow & Niels Ferguson, On the Possibility of a Back Door in the NIST SP800-90 Dual EC Prng 8, Presentation at the 27th Annual International Cryptology Conference (Aug. 21, 2007), https://rump2007.cr.yp.to/15-shumow.pdf [https://perma.cc/ZF26-4HQS]. In fact, the Canadian company Certicom had filed a patent application on the backdoor in Dual_EC_DRBG in 2005, but Certicom never publicized this information. *Certicom's Patent Applications Regarding Dual EC Key Escrow*, PROJECT BULLRUN (July 29, 2005), https://projectbullrun.org/dual-ec/patent.html [https://perma.cc/WR7C-V8MP].

[12] Shumow & Ferguson, *supra* note 11, at 7.

[13] In March 2006, Kristian Gjøsteen sent a paper to the National Institute of Standards and Technology (NIST) showing that the bit strings output from Dual_EC_DRBG were biased. Kristian Gjøsteen, Comments on Dual-EC-DRBG/NIST SP 800-90 (Dec. 2005) (unpublished manuscript). This was later improved by Berry Schoenmakers and Andrey Siderenko. Berry Schoenmakers & Andrey Siderenko, *Cryptanalysis of the Dual Elliptic Curve Pseudorandom Generator* 1 (2006) (manuscript), 2006 CRYPTOLOGY EPRINT ARCHIVE, https://eprint.iacr.org/2006/190.pdf [https://perma.cc/6QUQ-MCB4]. Both of these papers were out after the NIST deadline for comments but before NIST had completed editing the standard. Daniel Bernstein, Tanja Lange & Ruben Niederhagen, *Dual EC: A Standardized Backdoor*, *in* THE NEW CODEBREAKERS: ESSAYS DEDICATED TO DAVID KAHN ON THE OCCASION OF HIS 85TH BIRTHDAY 256, 260 (Peter Y.A. Ryan, David Naccache, & Jean-Jacques Quisquater eds., 2016).

[14] Beginning in 2006, there were several technical papers showing the potential for backdoors and other problems with the system. *See* Shumow & Ferguson, *supra* note 11, at 8; SCHOENMAKERS & SIDERENKO, *supra* note 13, at 1; *infra* Part I.A.

[15] ELAINE BARKER & JOHN KELSEY, NAT'L INST. OF STANDARDS & TECH., NIST SPECIAL PUBLICATION NO. 900-80A REV. 1, RECOMMENDATION FOR RANDOM NUMBER GENERATION USING DETERMINISTIC RANDOM BIT GENERATORS 58 (2006), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90Ar1.pdf [https://perma.cc/Q66G-SVHC].

[16] FIPS are developed by NIST for use in computer systems for non-national security agencies of the U.S. government. For further information on FIPS, see *Compliance FAQs: Federal Information Processing Standards (FIPS)*, NAT'L INST. OF STANDARDS & TECH.

security agencies of the federal government. Although FIPSs only apply to federal non-national security agencies, the impact of the designation is far broader. FIPSs are often adopted by industries, including those outside the United States, for private sector use. That NIST had designated a corrupted cryptosystem as a FIPS thus had reverberations well beyond U.S. borders.

The problem of the algorithm was quickly handled. NIST, which had approved[17] Dual_EC_DRBG as a FIPS, immediately responded by recommending that the algorithm not be used and opened a public comment period on the standard.[18] Seven months later, NIST permanently removed Dual_EC_DRBG from its list of recommended random-number generators.[19] The problem of reestablishing NIST as a purveyor of widely used cryptographic standards—a role it had been successfully filling—was more complex.

This situation provides a conundrum. The Snowden disclosure of a cryptographic backdoor in Dual_EC_DRBG revealed, at best, a weakness in the NIST process of developing cryptographic standards. At worst, it showed nefarious intent on the part of the U.S. government agency. Yet within just a short period it became clear that NIST's Computer Security Division (CSD) was able to successfully continue as a largely trusted developer of internationally accepted cryptographic standards, most recently with its efforts to develop post-quantum cryptographic standards[20] and lightweight cryptography for the Internet of Things and cyber-physical systems.[21]

(Nov. 15, 2019), https://www.nist.gov/standardsgov/compliance-faqs-federal-information-processing-standards-fips [https://perma.cc/4W6U-AP5P].

[17] BARKER & KELSEY, *supra* note 15, at 100.

[18] *NIST Removes Cryptography Algorithm from Random Number Generator Recommendation*, NAT'L INST. OF STANDARDS & TECH. (Apr. 21, 2014), https://www.nist.gov/news-events/news/2014/04/nist-removes-cryptography-algorithm-random-number-generator-recommendations [https://perma.cc/HA3P-NW5B].

[19] *Id*.

[20] *Post-Quantum Cryptography (PQC),* NAT'L INST. OF STANDARDS & TECH. (Jan. 3, 2017), https://csrc.nist.gov/projects/post-quantum-cryptography [https://perma.cc/AQ96-GZU9]. Public-key cryptographic algorithms are believed to be strong and effective against attacks by classical computers, but in 1994 Peter Shor showed a quantum algorithm can factor integers into prime factors much faster than any known classical algorithm. With a major scientific advancement in quantum computing, it might be possible to crack a communication encrypted through current public-key means in a matter of hours. *See* Peter W. Shor, *Algorithms for Quantum Computation: Discrete Logarithms and Factoring*, 1994 PROC. 35TH ANN. SYMP. FOUND. COMPUTER SCI. 124 (1994).

[21] *Lightweight Cryptography*, NAT'L INST. OF STANDARDS & TECH. (Jan. 3, 2017), https://csrc.nist.gov/Projects/lightweight-cryptography [https://perma.cc/D8YE-ZJU4].

In this paper we explain this conundrum. We begin, in Part I, by providing context through a short primer on cryptography and on NIST's role in developing cryptographic standards. In Part II, we discuss what NIST did to address the problems that allowed a problematic algorithm to be approved as a FIPS and the reaction of the international cryptography community. We next examine in Part III why the situation resolved in this way.

Yet the story does not end with NIST's successful regaining of the international cryptographic research community's trust. The Dual_EC_DRBG situation played out against a nearly forty-year continuing conflict between the U.S. government and cryptographers and computer security experts and a fifteen-year history of cooperation between NIST and the cryptographic research community. In Part IV, we briefly discuss the stability of this resolution against two sets of changes: the role of the U.S. in Europe and elsewhere and the increasing fragmentation of the Internet.

I. CRYPTOGRAPHY: A COMPLEX TECHNOLOGY WITH COMPLEX POLICY ISSUES

Cryptography has a long history; encryption was used to obscure the meaning of a communiqué in almost every civilization in which there was writing.[22] For centuries, though, encryption was an obscure topic, largely the domain of generals, diplomats, and young children.[23] In the 1970s, academic researchers, anticipating the revolution that the Internet would make in communications, began to explore encryption.[24] That change was alarming to the NSA, which had been accustomed to owning all things cryptographic, both the design of cryptographic systems and the development of cryptanalytic techniques to breach them. The conflict over encryption—the Crypto Wars of both the last century and this one—have been discussed in

[22] In 1500 B.C., for example, a Mesopotamian scribe describing glazes for pottery "encrypted" his technique by using cuneiform with different syllabic interpretations. *See* DAVID KAHN, THE CODEBREAKERS: THE COMPREHENSIVE HISTORY OF SECRET COMMUNICATION FROM ANCIENT TIMES TO THE INTERNET 75 (1996). As Kahn points out, this spelling method is much like the way George Bernard Shaw proposed spelling "fish" as "ghoti" (the "gh" as in "tough," the "i" as in "women," and the "ti" as in "nation"). *Id*. The Kama Sutra lists secret writing as a skill women should know. *Id*. at 74.

[23] The discussion of use by the military and diplomats runs through David Kahn's tour de force on the history of cryptography. *See generally id*. Children also frequently use secret codes. *See generally* IONA & PETER OPIE, THE LORE AND LANGUAGE OF CHILDREN (1959); Rochelle Berkovits, *Secret Languages of Schoolchildren*, 26 N.Y. FOLKLORE Q. 127 (1970).

[24] *See, e.g.*, Whitfield Diffie & Martin E. Hellman, *New Directions in Cryptography*, 22 IEEE TRANSACTIONS INFO. THEORY 644, 644 (1976), https://ee.stanford.edu/~hellman/publications/24.pdf [https://perma.cc/H7FM-USZM].

great detail elsewhere,[25] and thus there is no need to do so here. Instead we limit ourselves to the background necessary to understand the Dual_EC_DRBG issue: a short discussion on cryptographic systems and a recap of the policy conflict between the NSA and NIST over the development of cryptographic standards for non-national security agencies of the U.S. government.

A. A Primer on Cryptographic Systems

Cryptography is used to encode communications and data so that only the intended users of the information are able to access the decrypted version. A cryptographic system relies on an algorithm, a method for encrypting data (communications or data in storage), and a key—a parameter used by the algorithm. It is a well-accepted principle in cryptography that the algorithm—the method of encryption—should be public.[26] This allows vetting of the system. Meanwhile the encryption key should remain private to the users who are communicating.[27] The security of a user's encrypted message or data relies on keeping her encryption key secret. A cryptographic system is considered strong if nothing short of a brute-force search of all possible keys will enable decrypting encrypted data.

This paradigm—security lies in the key's secrecy—creates the challenge of key exchange: how do two users securely exchange their keys if their only form of communication is over an insecure channel? This is particularly problematic in situations in which the two endpoints, such as Amazon and a customer, have no prior relationship but are now communicating over an insecure network such as the Internet.

In 1976, Whitfield Diffie, Martin Hellman, and Ralph Merkle solved this problem by inventing *public-key cryptography*, which uses different keys for encryption and decryption: a *public* key that is widely disseminated and a *private* key that only the owner knows.[28] The sender encrypts by applying the

---

[25] *See, e.g.*, WHITFIELD DIFFIE & SUSAN LANDAU, PRIVACY ON THE LINE: THE POLITICS OF WIRETAPPING AND ENCRYPTION (2007); Harold Abelson, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Whitfield Diffie, John Gilmore, Matthew Green, Susan Landau, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller, Bruce Schneier, Michael A. Specter & Daniel J. Weitzner, *Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications*, 1 J. CYBERSECURITY 69 (2015).

[26] Auguste Kerckhoffs, *La Cryptograhie Militaire [Military Cryptography]*, 9 J. DES SCIENCES MILITAIRES 1, 5 (1883).

[27] *Id*.

[28] Diffie & Hellman, *supra* note 24, *passim*; Ralph C. Merkle, *Secure Communications Over Insecure Channels*, 21 COMM. ACM 294, 294 (1978).

encryption algorithm and the recipient's public key to the message; the recipient, who is the only one who knows the private key, decrypts the encrypted message. Two early public-key algorithms—Diffie-Hellman and the Rivest, Shamir, and Adleman (RSA) algorithm[29]—are widely deployed. In the 1980s, an alternative algorithm for public-key cryptography, elliptic curve cryptography (ECC),[30] was proposed. ECC's advantage over Diffie-Hellman and RSA is in providing the same level of protection as the earlier methods but at much shorter key lengths, thus using less storage and power.[31] ECC's lower power makes the method particularly useful for power-constrained devices such as mobile phones and IoT devices.

Public-key systems are sometimes known as asymmetric encryption since the encryption and decryption keys are different; other systems, such as the Advanced Encryption Standard (AES), use the same key for encryption and decryption and are known as symmetric encryption systems. Public-key systems are generally computationally slower than their symmetric-key counterparts and are thus typically used only for transmitting encryption keys. The actual encryption is usually done by symmetric-key systems. Cryptography enables protections, including providing confidentiality, integrity, and authenticity. Integrity is provided through tools such as hash functions, easy-to-compute compression functions that transform variable-length inputs to short length outputs. Digital signatures[32] can ensure the authenticity of a digital communication.

All types of encryption functions depend on keys. A decryption key should not only be secret, but it should also be unguessable. That means the key bits should be unpredictable, that is, computationally impossible to

---

[29] Ronald Rivest, Adi Shamir & Leonard Adleman, *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*, 21 COMM. ACM 120, 120–21 (1978). The Diffie-Hellman key exchange and the RSA encryption system, but not digital signatures, were apparently discovered earlier by James Ellis, Clifford Cocks, and Malcolm Williamson of the U.K.'s Government Communication Headquarters (GCHQ) in the early 1970s. J.H. Ellis, *The History of Non-Secret Encryption*, 23 CRYPTOLOGIA 267, 268 (1999). The work was classified, and the discovery was only made public in 1997. GCHQ did not see the work's potential, and it was not followed up. *Id.*

[30] This idea was discovered independently by Neal Koblitz and Victor Miller. Neal Koblitz, *Elliptic Curve Cryptosystems*, 48 MATHEMATICS COMPUTATION 203, 203–04 (1987); Victor Miller, *Use of Elliptic Curves in Cryptography*, *in* ADVANCES IN CRYPTOLOGY—CRYPTO '85 PROCEEDINGS 417–18 (Hugh C. Williams ed., 1986).

[31] Arjen K. Lenstra & Eric R. Verheul, *Selecting Cryptographic Key Sizes*, 14 J. CRYPTOLOGY 255, 268 (2001).

[32] Digital signatures were invented by Whitfield Diffie and Martin Hellman. Diffie & Hellman, *supra* note 24.

distinguish from unbiased or random bits.[33] This presents a different problem for creating keys.[34] While physical processes can produce random bits, they are too slow for the number of keys needed as the number of encrypted communications vastly increased. Cryptographers looked to the ideas of "pseudo-random-number generators" (PRNG), functions that take a short random sequence of numbers (or bits), typically taken from a random physical process (including from within a computer), and produce a much longer sequence that is computationally indistinguishable from a random one.[35] In the early 2000s, the American National Standards Institute (ANSI) proposed using elliptic curves to produce PRNGs.[36] But the method proposed, Dual_EC_DRBG, had a weakness, one that would later be revealed by the Snowden disclosures. NSA had built a backdoor into commercial encryption products, cleverly manipulating the cryptographic standardization process to enable wide deployment of the system.

B. Standardization and Dual_EC_DRBG

To go from a mathematical formulation of an encryption method or random-number generator to its implementation in widely used software requires that the algorithm become a standard. The process of standardizing a cryptographic algorithm is intended to ensure trust in approved standards. It is the *sine qua non* of the cryptographic world; a cryptographic algorithm or random-number generator that is not a standard is a mathematical curiosity, not a technique that should be used in products.[37] Standardization

---

[33] ELAINE BARKER, ALLEN ROGINSKY & RICHARD DAVIS, NAT'L INST. OF STANDARDS & TECH., NIST SPECIAL PUBLICATION 800-133 REV. 2, RECOMMENDATION FOR CRYPTOGRAPHIC KEY GENERATION 7, 11 (2020), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-133r2.pdf [https://perma.cc/UZ5X-CNHH].

[34] This is an old problem in encryption; failing to do it well can lead to spectacular failures. Systems using one-time pads, in which the encryption key is as long as the message, are essentially unbreakable if the key is (1) truly random and (2) never reused. But during World War II, the Soviet cryptographic office reused keys—allowing the NSA to break encrypted communications a decade later. *See* JOHN EARL HAYNES & HARVEY KLEHR, VENONA: DECODING SOVIET ESPIONAGE IN AMERICA 29 (1999); *Venona Documents*, NAT'L SEC. AGENCY, https://www.nsa.gov/Helpful-Links/NSA-FOIA/Declassification-Transparency-Initiatives/Historical-Releases/Venona/ [https://perma.cc/X87V-UU98] (last visited Feb. 15, 2022).

[35] More precisely, this means that no polynomial-time test—a test that runs in polynomial time (n^c, where n is the size of the input string to the generator measured in bits and c is a constant)—can distinguish the pseudo-random bit string from a truly random one.

[36] Bernstein, Lange & Niederhagen, *supra* note 13, at 262.

[37] Cryptographers describe cryptographic algorithms that are not open to public vetting as "snake oil."

precisely specifies the algorithm and the form the input and output must take. Such standardization ensures that different implementations are compatible and thus interoperable.

Two characteristics are necessary for an algorithm to become a cryptographic standard. First, it must function well, which is to say, be cryptographically strong and capable of being used for a long period of time. Second, a standard must be publicly evaluated. But through manipulating the process and presenting half-truths at various points,[38] the NSA "finessed" the approval process for Dual_EC_DRBG that, though nominally public, largely avoided scrutiny by cryptographic researchers.[39]

In the early 2000s, the NSA first arranged to standardize Dual_EC_DRBG at ANSI and the International Standards Organization (ISO).[40] This was a clever move. Academic cryptographers play a large role in evaluating proposed cryptographic standard submissions to NIST, but not so at ANSI, which is a pay-to-play standardization organization. The price for membership is sufficiently high that ANSI has few university members. ISO membership is limited to national standards bodies, thus also effectively eliminating academic participation. In having the Dual_EC_DRBG standardization process start with ANSI and ISO prior to bringing the algorithm to NIST, the NSA had skillfully avoided early public examination of Dual_EC_DRBG.[41]

NIST plays a unique and unusual role within the U.S. government. A non-regulatory agency, its purpose is promoting "U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology."[42] Such a description runs the risk of sounding mundane; however, the impact of its work is anything but. Precise measurement—knowing how to measure, test, and ensure the interoperability of new technologies—is important to moving an initial prototype of an innovative technology to a successful product. At the same time, though NIST's *raison*

---

[38] Daniel Bernstein, Tanja Lange & Ruben Niederhagen, *supra* note 13, at 256.

[39] Pelroth et al., *supra* note 7 (describing classified NSA memo about the standard's approval, which stated that the effort was "a challenge in finesse"). A carefully documented description of the steps the NSA took can be found in Bernstein, Lange & Niederhagen, *supra* note 13, at 256.

[40] Bernstein, Lange & Niederhagen, *supra* note 13, at 262–63.

[41] There were, nonetheless, technical criticisms of the security of the proposed standard submitted by several researchers during the NIST standardization effort. *Id.* at 256.

[42] *NIST Mission, Vision, Core Competencies, and Core Values*, NAT'L INST. OF STANDARDS & TECH. (July 10, 2009), https://www.nist.gov/about-nist/our-organization/mission-vision-values [https://perma.cc/4AWD-TG78].

d'etre is benefiting U.S. innovation and industrial competitiveness,[43] that does not mean putting U.S. companies first. Indeed, the situation is quite to the contrary; NIST is seen by industry as an "honest broker"[44] that favors neither a particular company nor a country. By conducting unbiased assessments, NIST functions as a trusted player in the world of international industrial standards. NIST also serves a valuable role as the developer of FIPS, a role not shared by ANSI, ISO, or any other standards organization. The NSA's pressure on NIST to approve Dual_EC_DRBG as a FIPS was a crucial aspect of the NSA's "finessing" of the standard.

NIST's effort to develop recommendations for random-number generators started shortly after the work at ANSI and ISO; as a result, NIST's work relied on the standardization efforts done in these other venues. Such a workflow was not unusual for the Department of Commerce agency, which has always aimed to play well with others, a useful behavior in the standards world. Dual_EC_DRBG was proposed during a 2004 NIST workshop on random-number generation.[45] In fact, most proposals at the NIST workshop came from submissions to the ANSI effort, which was further along.[46] But

---

[43] *Id*.

[44] Carl Cargill, Director, Corporate Standards, Sun Microsystems, described NIST as the "impartial, empowered, and very competent observer" in standards coordination, contrasting the agency with other consortia, in which "there was always the question of what is in it for them." Constance Morella then responded, "I like the language you used, [NIST as a] well-credentialed, honest broker." *The Role of Technical Standards in Today's Society and in the Future: Hearing Before the Subcomm. on Tech. of the H. Comm. on Sci.*, 106th Cong. 125–26 (2000), https://babel.hathitrust.org/cgi/pt?id=umn.31951p007015881&view=1up&seq=2&skin=2021 [https://perma.cc/KT8A-RQ7X]. Two years later, Representative Sherwood Boehlert, chair of the House Science Committee, used the words "honest broker" to describe NIST. *HR 5005, The Homeland Security Act of 2002, Day 3: Hearing Before the H. Select Comm. on Homeland Sec.*, 107th Cong. 143 (2002) (statement of Rep. Sherwood Boehlert, Chairman, H. Comm. on Sci.), https://www.govinfo.gov/content/pkg/CHRG-107hhrg83173/pdf/CHRG-107hhrg83173.pdf [https://perma.cc/Q38V-Z278].

[45] Don Johnson, an employee at Entrust, a Canadian company producing identity-management software, presented Dual_EC_DRBG at a 2004 NIST workshop on random number generation. *See* Don Johnson, X9.82 Part 3 Number Theoretic DRBGs, Presentation at the National Institute of Standards and Technology (NIST) RNG Workshop, 23 (2004), https://csrc.nist.gov/csrc/media/events/random-number-generation-workshop-2004/documents/numbertheoreticdrbg.pdf [https://perma.cc/89J4-2HDD]. The algorithm was already under consideration as a standard for generating pseudo-random bits at ANSI, the American National Standards Institute. Bernstein, Lange & Niederhagen, *supra* note 13, at 260.

[46] JOHN KELSEY, NAT'L INST. OF STANDARDS & TECH., DUAL EC IN X9.82 AND SP 800–90 12–16 (2014) https://csrc.nist.gov/csrc/media/projects/crypto-standards-development-process/documents/dualec_in_x982_and_sp800-90.pdf [https://perma.cc/KDX7-UUZE].

there was a problem with this model: contrary to usual NIST processes, many of the proposals open for public review were actually "not very public."[47]

Dual_EC_DRBG was peculiar, both because it was very slow (several orders of magnitude slower than other random-number generators) and the way it was designed. Researchers raised concerns to NIST about both possible bias in the bits[48] and a possible backdoor[49] in Dual_EC_DRBG.[50] NIST examined the issue.[51] NSA dismissed NIST's concerns, responding that implementers could choose their own parameters to handle concerns about possible backdoors.[52] NSA pressed NIST to standardize the algorithm, claiming that it needed FIPS validation of agency devices running Dual_EC_DRBG,[53] and thus NIST approved Dual_EC_DRBG as one of four possible standardized random-bit generators.[54] Dual_EC_DRBG remained a FIPS until shortly after the 2013 revelation of an NSA backdoor in a cryptographic algorithm.

Documents disclosed by Edward Snowden revealed that NSA had "[i]nsert[ed] vulnerabilities into commercial encryption systems" and "[i]nfluence[d] policies, standards, and specification for commercial public key technologies."[55] Suspicion immediately fell on Dual_EC_DRBG.[56] A backdoor would give the agency—or anyone else who knew it—a way to efficiently calculate the so-called random bits, thus removing the security of the key and anything encrypted with it. NIST reacted quickly to a September 2013 *New York Time*s story regarding Dual_EC_DRBG.[57] Just five days after the article appeared, NIST announced it was reopening commenting on the standard.[58] That month, NIST issued a Supplemental ITL Bulletin strongly

---

[47] *Id.* at 15.
[48] *See* discussion, *supra* note 13.
[49] *See* discussion, *supra* note 11.
[50] Bernstein, Lange & Niederhagen, *supra* note 13, at 260–61, 263.
[51] One problem was that NIST asked whether the algorithm had been corrupted—they found no evidence of this—rather than whether it could be. KELSEY, *supra* note 46, at 27.
[52] *Id*.
[53] *Id*.
[54] BARKER & KELSEY, *supra* note 15.
[55] *Secret Documents*, *supra* note 8.
[56] Dual_EC_DRBG was a random number generator that provided bits for an encryption key; the backdoor enabled anyone with secret knowledge to quickly calculate those bits.
[57] Reports also appeared in the *Guardian* and *ProPublica*. *See* Ball, Borger & Greenwald, *supra* note 7; Larson, *supra* note 7.
[58] *Cryptographic Standards Statement*, NAT'L INST. OF STANDARDS & TECH. (Sept. 10, 2013), https://www.nist.gov/news-events/news/2013/09/cryptographic-standards-statement [https://perma.cc/HD84-B34D].

recommending against the use of Dual_EC_DRBG until its security issues had been resolved.[59]

C. NSA, NIST, and Cryptographic Standards: A Complicated Relationship

The 1965 *Brooks Act*[60] gave the National Bureau of Standards the role of developing "scientific and technological advisory services relating to automatic data processing."[61] In the early 1970s, the U.S. government realized it needed a cryptographic standard for securing sensitive data held by non-national security government agencies. NSA, which was the obvious candidate to produce such an algorithm, was unwilling to have its techniques for cryptographic design become public. The National Bureau of Standards (NBS), renamed the National Institute of Standards and Technology (NIST) in 1988,[62] was tasked with soliciting proposals for a cryptographic standard.[63] For simplicity, we will refer to the agency as NIST from hereon in.

When in 1973 NIST issued a request for proposals for a cryptographic algorithm to secure data—the Data Encryption Standard (DES)—NIST lacked even a single cryptographer on staff. NSA, as the agency with sufficient expertise, had to evaluate the submissions.[64] At the time, the use of cryptography was nascent in the private sector, with few companies having cryptographic expertise. IBM, which had been developing cryptographic systems for the banking industry, had a cryptography research group—and

---

[59] *Supplemental ITL Bulletin for September 2013*, NAT'L INST. OF STANDARDS & TECH. (Sept. 2013), https://csrc.nist.gov/CSRC/media/Publications/Shared/documents/itl-bulletin/itlbul2013-09-supplemental.pdf [https://perma.cc/HMP3-4GPM].

[60] Pub. L. No. 89-306 (1965).

[61] INST. FOR COMPUT. SCIS. & TECH., NAT'L BUREAU OF STANDARDS, A TEN YEAR HISTORY OF THE NATIONAL BUREAU OF STANDARDS AND ACTIVITIES UNDER THE BROOKS ACT (PUBLIC LAW 89-306) 2 (1977) https://www.govinfo.gov/content/pkg/GOVPUB-C13-3e65f18fd63b6ba185f07afaf1427c99/pdf/GOVPUB-C13-3e65f18fd63b6ba185f07afaf1427c99.pdf [https://perma.cc/WQ7T-QBMK].

[62] The National Bureau of Standards became known as the National Institute of Standards and Technology as a result of the Omnibus Trade and Competitiveness Act of 1988, Pub. L. No. 100-418, §§ 5112(a), 5115 (1998).

[63] Cryptographic Algorithms for Protection of Computer Data During Transmission and Dormant Storage, 38 Fed. Reg. 12,763 (May 15, 1973).

[64] THOMAS JOHNSON, CTR. FOR CRYPTOLOGICAL HISTORY, NAT'L SEC. AGENCY, AMERICAN CRYPTOLOGY DURING THE COLD WAR: 1945-1989; BOOK III: RETRENCHMENT AND REFORM: 1972-1980 232 (1998) https://www.nsa.gov/portals/75/documents/news-features/declassified-documents/cryptologic-histories/cold_war_iii.pdf [https://perma.cc/EGL9-B73Y].

the company responded to NIST's call.[65] A modified version of IBM's submission was approved as DES.[66] DES was approved as a FIPS, which meant it would be in computer equipment sold to non-national security federal agencies. The result was that DES was broadly implemented in computer equipment used by industry and sometimes by foreign governments.

Controversies arose out of DES's relatively short key length and NSA's involvement in the DES evaluation process.[67] The lack of transparency in the algorithm selection process raised further doubts regarding the algorithm's strength. Decades later, an internal history of NSA confirmed that NSA pressure had indeed forced adoption of a 56-bit key for DES instead of a stronger 64-bit key sought by IBM.[68]

With rising tension in the 1980s over President Reagan's order to safeguard "sensitive, but unclassified" information in executive branch and its contractors' communications and computer systems,[69] some in Congress felt that the executive branch policy was intruding on legislative turf.[70] The congressional response was the 1987 *Computer Security Act*,[71] which explicitly made NIST responsible for "developing standards and guidelines for Federal computer systems," including cryptography. But the Act had a caveat—NIST was to use NSA for "technical advice and assistance."[72] This provision granted NSA significant control over NIST's development of cryptographic standards.

---

[65] *Cryptography for a Connected World*, IBM, https://www.ibm.com/ibm/history/ibm100/us/en/icons/cryptography/ [https://perma.cc/2M8W-JHTT] (last visited Dec. 10, 2021).

[66] JOHNSON, *supra* note 64, at 232.

[67] *Id.* at 232–33; *see also* STAFF OF S. SELECT COMM. ON INTELLIGENCE, 95TH CONG., UNCLASSIFIED SUMMARY: INVOLVEMENT OF NSA IN THE DEVELOPMENT OF THE DATA ENCRYPTION STANDARD 2–3 (Comm. Print 1978), https://www.intelligence.senate.gov/sites/default/files/publications/95nsa.pdf [https://perma.cc/27EV-A4H6].

[68] JOHNSON, *supra* note 64, at 232.

[69] National Policy on Telecommunications and Automated Information Systems Security, National Security Decision Directive 145 (Sept. 17, 1984), https://irp.fas.org/offdocs/nsdd145.htm [https://perma.cc/PH7A-T4CX].

[70] DIFFIE & LANDAU, *supra* note 25, at 75.

[71] Computer Security Act of 1987, Pub. L. No. 100-235, § 2(b)(1) (1988). The Act initially made NBS responsible for cryptography. *Id.* Subsequent statutes have amended the Act to clarify that NIST, NBS's successor organization, is responsible for cryptography. *See* 40 U.S.C. § 1441(a).

[72] *Id.*

As policy scholar Michael Ting has observed, "legislation is an 'incomplete contract' for controlling the bureaucracy."[73] The Act said NIST was to consult NSA for "technical advice and assistance," but what did that mean in practice? In 1989, the two agencies signed a Memorandum of Understanding (MOU) establishing the roles of the two agencies under the new law.[74] It was quite deferential to NSA. In retrospect, this should not be fully surprising; NSA had technical expertise in cryptography, NIST did not. Indeed, NIST's CSD was chronically underfunded for decades.[75] An additional twist was that, as Whitfield Diffie and Susan Landau noted in 1998, NIST Director Raymond Kammer, who was the son of two NSA employees, "was deeply concerned about protecting national-security and law-enforcement interests in cryptography."[76] The MOU provided NSA with more control over cryptographic standards than the Computer Security Act appears to have intended.

The MOU established a six-person Technical Working Group (TWG)—three from each agency.[77] But while there was balance in representation, there was imbalance in the appeals process. Disputes could be elevated to the Secretary of Defense and the Secretary of Commerce;[78] in such an instance, the Department of Defense's viewpoint was extremely likely to trump the Department of Commerce's due to the DoD's national security mission. In several disputes, including over a standard for digital signatures[79] and over putting forth the Escrowed Encryption Standard ("Clipper") as a FIPS, NSA members of the TWG overrode objections of NIST members.[80] The internal fights of the TWG, and the frequent override

---

[73] Michael M. Ting, *Organizational Capacity*, 27 J. L. ECON. & ORG. 245, 246–47 (2011).

[74] 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, 2–4 (Mar. 24, 1989), https://csrc.nist.gov/CSRC/media/Projects/Crypto-Standards-Development-Process/documents/NIST_NSA_MOU-1989.pdf [https://perma.cc/8RJE-4NRP] [hereinafter 1989 NIST-NSA Memorandum of Understanding].

[75] *See* INFO. SEC. & PRIV. ADVISORY BD., NAT'L INST. OF STANDARDS & TECH., THE CASE FOR ADEQUATE FUNDING 6 (2004), https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/correspondence/ISPAB-ReportAdequateFundingNIST-CSD.pdf [https://perma.cc/ZXT6-C54E]. Susan Landau was on the Information Security and Privacy Advisory Board during the writing of this report.

[76] DIFFIE & LANDAU, *supra* note 25, at 78–79. This excerpt is based on an interview by Susan Landau and Raymond Kammer conducted on December 19, 1996.

[77] 1989 NIST-NSA Memorandum of Understanding, *supra* note 74, at 3, ¶ 5.

[78] *Id.* at 4.

[79] A digital signature is a mathematical function that enables a user to verify the authenticity of digital messages.

[80] Susan Landau, *Under the Radar: NSA's Efforts to Secure Private-Sector Telecommunications Infrastructure*, 7 J. NAT'L SEC. L. & POL'Y 411, 411 (2014).

of NIST by NSA, were largely unknown publicly. The public and, most critically, the cryptographic research community, were thus largely unaware of NIST's fights for strong cryptography for public use.[81]

A significant transformation of these dynamics came with a change in personnel within the TWG. The NSA-NIST MOU established the NSA Deputy Director for Information Security as the point of contact for this working group, but NSA had filled the position with a member of the signals intelligence (SIGINT) community.[82] This led to a different focus than the law had perhaps intended. The main goal of NSA's Information Assurance Directorate (IAD), the successor to the Information Systems Security Organization, was to secure information; SIGINT's role was to access it. In September 1997, IAD's technical director, Brian Snow, became the TWG co-chair. For anyone watching closely, this action hinted at changes emanating from NSA.

By 1997, it was clear that DES was reaching the end of its utility; a 56-bit encryption algorithm was no match for machines that could do a brute-force search of the key space.[83] That year, NIST put out a call for proposals to develop an algorithm with much longer key lengths—128-, 192-, and 256-bits—to replace DES.[84] In contrast to the 1970s call for a data encryption algorithm,[85] this time NIST's actions were highly transparent. It began with a call for comments on proposed criteria of the proposed standard[86]—with the

---

[81] The NIST Technical Group members sought to include RSA as a digital signature standard, and the NSA members of the TWG opposed it. The NIST members of the TWG were overridden by Kammer, who deferred to NSA members' recommendation. DIFFIE & LANDAU, *supra* note 25, at 347 n.36.

[82] Landau, *supra* note 80, at 427.

[83] This was due to a challenge launched by RSA Laboratories; key recovery, which was done in 96 days, was accomplished through linking together thousands of computers online. *See* Matt Curtin & Justin Dolske, *A Brute Force of DES Keyspace*, INTERHACK (May 1998), http://web.interhack.com/publications/des-key-crack [https://perma.cc/G64S-54BB]. A year later, Cryptography Research, Inc., Advanced Wireless Technologies, and the Electronic Frontier Foundation spent $250,000 on a special-purpose machine for searching the DES keyspace; they cracked DES-encrypted message in 56 hours. *See generally* ELEC. FRONTIER FOUND., CRACKING DES: SECRETS OF ENCRYPTION RESEARCH, WIRETAP POLITICS. & CHIP DESIGN (1998) (describing how to build a DES cracker).

[84] Announcing Request for Candidate Algorithm Nominations for the Advanced Encryption Standard, 62 Fed. Reg. 48,051, 48,051–58 (Sept. 12, 1997).

[85] Cryptographic Algorithms for Protecting Computer Data During Transmission and Dormant Storage: Solicitation of Proposals, 38 Fed. Reg. 12,763, 12,763 (May 15, 1973).

[86] Announcing Request for Candidate Algorithm Nominations, *supra* note 84, at 48,051–58.

criteria fully determined only after a public workshop several months later.[87] At the time that NIST issued the call for developing an Advanced Encryption Standard (AES), it was not clear that the agency had sufficient technical expertise to play a leading role in such an endeavor.[88] NIST understood that any successful encryption standard would need participation of the international cryptographic community. When the academics largely failed to attend the initial workshop on evaluation and submission requirements held at NIST, the agency opted to hold future meetings alongside academic conferences.[89]

NIST worked with the cryptographic community to revolutionize the process of the algorithm selection so that it became a truly international effort. The process that NIST used in developing AES was sufficiently successful that the agency later institutionalized it. Cryptographers from around the world were involved at each stage of the process—from the call for proposals to each round of assessing the security of the submitted algorithms.[90] NIST, as an unbiased arbiter, ran competitions and released reports that summarized findings for the stages of the process.[91] Researchers published their attacks on the submissions. Such an open vetting process was critical; subtle changes in an algorithm can vastly change its security.[92] Only careful study by experts can reveal such problems.

---

[87] Miles E. Smid, *Development of the Advanced Encryption Standard*, 126 J. RSCH. NAT'L INST. STANDARDS & TECH. 1, 1 (2021), https://nvlpubs.nist.gov/nistpubs/jres/126/jres.126.024.pdf [https://perma.cc/F45G-VPHY].

[88] *Id.* at 5.

[89] *Id.* at 1.

[90] *See id.* at 8; Edward Roback & Morris Dworkin, *Conference Report: First Advanced Encryption Standard (AES) Candidate Conference, Ventura, CA August 20-22, 1998*, 104 J. RSCH. NAT'L INST. STANDARDS & TECH. 97, 97 (1999), https://www.proquest.com/docview/214775939/fulltextPDF/44126024D94840B3PQ/1?accountid=15159 [https://perma.cc/DKF3-EW72]; Morris Dworkin, *Second Advanced Encryption Standard Candidate Conference, Rome, Italy March 22-23, 1999*, J. RSCH. NAT'L INST. STANDARDS & TECH. 401, 401 (1999), https://nvlpubs.nist.gov/nistpubs/jres/104/4/j44ce-dwo.pdf [https://perma.cc/Q5AT-M4DL].

[91] Roback & Dworkin, *supra* note 90, at 98–99; Dworkin, *supra* note 90, at 402–04.

[92] Ronald Rivest, *Preliminary Findings Regarding NIST's Development of Cryptographic Materials*, *in* NAT'L INST. OF STANDARDS & TECH., NIST CRYPTOGRAPHIC STANDARDS AND GUIDELINES DEVELOPMENT PROCESS: REPORT AND RECOMMENDATIONS OF THE VISITING COMMITTEE ON ADVANCED TECHNOLOGY OF THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (2014), https://www.nist.gov/system/files/documents/2017/05/09/VCAT-Report-on-NIST-Cryptographic-Standards-and-Guidelines-Process.pdf [https://perma.cc/R2ZM-XG6Q].

Unlike the 1970s, when IBM was an outlier in having cryptographic capabilities, most major technology companies in the U.S. and abroad had a unit responsible for implementing cryptography by the late 1990s; some also conducted cryptographic research. Cryptography research was well established in universities in North America, Europe, and Asia.[93] With this diffusion of expertise to non-state actors, NIST had a significantly larger pool of possible contributors than when it launched its call for DES. There were fifteen full submissions to the AES competition, only one of which had solely U.S. authorship.[94] NIST's effort to attract the international community, which included holding one evaluation meeting in Rome, worked. The chosen algorithm, Rijndael, an algorithm designed by two Belgian researchers,[95] was renamed Advanced Encryption Standard and approved as a FIPS in 2001.[96]

Meanwhile, NSA's interest in breaking cryptosystems was shifting. In the 1970s, NSA had been able to break many encryption systems around the world, but by the late 1990s, this situation was changing.[97] There were increasing numbers of bills in Congress intended to limit the export controls[98] that had largely prevented foreign use of U.S. computer and communications equipment with strong cryptographic systems.

---

[93] The first academic research conference in cryptography was CRYPTO, held in Santa Barbara, California in 1981and has been held annually since. Eurocrypt, more formally known as the Annual International Conference on the Theory and Applications of Cryptographic Techniques, was first held as a workshop in 1982; it has been held annually since 1984. Asiacrypt, now formally known as International Conference on the Theory and Application of Cryptology and Information Security, was held as Auscrypt in Australia in 1990, then changed its name to Asiacrypt in 1991 when it was held in Japan; it has been held annually in venues across Asia since then. *See generally* INT'L ASS'N FOR CRYPTOLOGIC RSCH., https://www.iacr.org [https://perma.cc/E8ZU-Q6J9] (last visited Jan. 15, 2022).

[94] Smid, *supra* note 87, at 1. Smid's paper lists four submissions—HPC, RC6, SAFER+, and Twofish—as from the United States, *id.*, but in fact, only HPC was designed solely by U.S. citizens. Susan Landau, *Communications Security for the Twenty-First Century: The Advanced Encryption Standard*, 47 NOTICES AM. MATHEMATICAL SOC'Y 450, 453 (2000).

[95] JOAN DAEMEN & VINCENT RIJMEN, AES PROPOSAL: RIJNDAEL 1 (1999), http://csrc.nist.gov/encryption/aes/rijndael [https://perma.cc/S8ZK-KY33].

[96] NAT'L INST. OF STANDARDS & TECH., FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION 197: ADVANCED ENCRYPTION STANDARD (AES) 1, 5 (2001), https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf [https://perma.cc/M2GK-R8K8].

[97] 145 CONG. REC. S8791 (daily ed. July 19, 1999) (statement of Sen. Kerrey).

[98] This included the Promotion of Commerce On-line in the Digital Era (PRO-CODE) bill in the Senate (S.377, 105th Cong. (1997)), the Security and Freedom Through Encryption (SAFE) Act in the House (H.R. 695, 105th Cong. (1997)), and the Promote Reliable On-Line Transactions to Encourage Commerce and Trade (PROTECT) Act in the Senate (S.798, 106th Cong. (1999)) in the 106th legislative session.

It was not clear that the controls, which hurt U.S. competitiveness, were that useful any longer. Increased use of submarine fiber-optic cables made NSA collection much more difficult.[99] Meanwhile increased strength of cryptosystems deployed by foreign governments made communications decryption more challenging.[100] A "recently retired" senior CIA officer told reporter Seymour Hersh in 1999 that, "The dirty little secret is that fiber optics and encryption are kicking Fort Meade [NSA headquarters] in the nuts."[101] Knowing the when and who of communications—the so-called communications "metadata"—could often be as useful as knowing the communications content,[102] and network exploitation became the agency's new priority. In exchange for Congress providing extra funding for this new priority, NSA backed off on the more stringent export controls. The agency opted for controls that enabled it to do its job but also enabled Silicon Valley to export many products with strong encryption.[103]

D. From Tension to Trust: NIST's Changing Relationship with the Cryptographic Research Community

Conflict between the U.S. government and the private sector over encryption policy arose in the 1970s over the publication of cryptography research.[104] It simmered in the 1980s, breaking out in full force in the 1990s

---

[99] Seymour Hersh, *The Intelligence Gap*, NEW YORKER (Dec. 6, 1999), https://www.newyorker.com/magazine/1999/12/06/the-intelligence-gap [https://perma.cc/JYK4-GTF9].

[100] *Id*.

[101] *Id*.

[102] Thus, for example, immediately after the attacks of September 11th, the U.S. government set up a secret program to collect U.S. bulk domestic communications metadata. This program was first revealed by *USA Today* in May 2006. Leslie Cauley, *NSA Has Massive Database of Americans' Phone Calls*, USA TODAY (May 11, 2006), https://usatoday30.usatoday.com/news/washington/2006-05-10-nsa_x.htm [https://perma.cc/6BF5-WT8F]. The program, which had originally begun under "presidential authority," was then authorized under Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, § 215, 115 Stat. 272, 287 (2001) (codified as amended at 50 U.S.C. § 1861(a)(1)). *See, e.g.*, NAT'L RSCH. COUNCIL, BULK COLLECTION OF SIGNALS INTELLIGENCE: TECHNICAL OPTIONS 20 (2015), https://www.nap.edu/catalog/19414/bulk-collection-of-signals-intelligence-technical-options [https://perma.cc/HY9K-8W9P].

[103] Landau, *supra* note 80, at 425.

[104] In 1979, NSA Director Bobby Inman warned that open publication of cryptography research was a threat to national security. *See, e.g., Report of the Public Cryptography Study Group*, Communications of the ACM, Vol. 24, No. 7 (July 1981), at 436.

over restrictions due to export controls and the introduction of the Clipper chip.[105]

Cryptography is a dual-use technology. During the Cold War, the technology was subject to export controls. The fall of the Soviet Union coincided with the time that U.S. industry began heavily pressuring the government to release those controls on cryptographic equipment (this was also the time just before the development of the public Internet). The 1990s marked a period of great public debate[106] on the E.U. and U.S. controls, which were greatly loosened in 2000.[107]

The Clipper chip, more formally known as EES,[108] was a symmetric-key system with an 80-bit key—and two controversial aspects. The encryption algorithm, Skipjack, was designed by NSA and was classified.[109] The encryption keys were to be split and escrowed with agencies of the U.S. government. The public first learned of Clipper in an April 1993 *New York Times* article;[110] public response was swift—and strongly opposed.[111] NSA sought to have EES approved as a FIPS, but public comment on the proposed standard—2 in favor, 318 opposed—was highly negative, with opposition

---

[105] Whitfield Diffie & Susan Landau, *The Export of Cryptography in the 20th and the 21st Centuries, in* THE HISTORY OF INFORMATION SECURITY: A COMPREHENSIVE HANDBOOK 725, 728–730 (Karl De Leeuw & Jan Bergstra eds., 2007).

[106] *Id.* at 725.

[107] *See* Revisions to Encryption Items, 65 Fed. Reg. 62,600, 62,601 (Oct. 19, 2000) (codified at 15 C.F.R. pts. 734, 740, 742, 770, 772, 774); Council Regulation (EC) 1334/2000, of 22 June 2000 Setting up a Community Regime for the Control of Exports of Dual-Use Items and Technology, 2000 O.J. (L 159) 1, 4. The U.S. then followed up with further loosening of controls. *See, e.g.*, Roszel C. Thomsen II & Antoinette D. Paytas, *US Encryption Export Regulation: US to EU:* Me *Too! — The United States Amends its Export Controls on Encryption, Responding to Recent Developments in the European Union*, 17 COMP. L. & SEC. REPORT 11, 11–12 (2001), https://doi.org/10.1016/S0267-3649(01)00103-0 [https://perma.cc/3PR6-QGWS].

[108] *See* NAT'L INST. OF STANDARDS & TECH., FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION 185: ESCROWED ENCRYPTION STANDARD 1, 2 (1994), https://csrc.nist.gov/csrc/media/publications/fips/185/archive/1994-02-09/documents/fips185.pdf [https://perma.cc/2H5U-EEXU] [hereinafter FIPS PUBLICATION 185].

[109] The algorithm was later declassified. OFF. OF ASSISTANT SEC'Y OF DEF., ENCRYPTION FORMULAS DECLASSIFIED (1998), https://irp.fas.org/news/1998/06/b06231998_bt316-98.html [https://perma.cc/6LCZ-ZR8D].

[110] John Markoff, *Electronics Plan Aims to Balance Government Access with Privacy*, N.Y. TIMES (Apr. 16, 1993), https://www.nytimes.com/1993/04/16/us/electronics-plan-aims-to-balance-government-access-with-privacy.html [https://perma.cc/L8MD-U2XB].

[111] Steven Levy, *Battle of the Clipper Chip*, N.Y. TIMES MAG. (June 12, 1994), https://www.nytimes.com/1994/06/12/magazine/battle-of-the-clipper-chip.html [https://perma.cc/MX9K-NQKX].

coming from cryptographers, computer security experts, civil-liberties groups, and the public.[112]

NIST nonetheless approved EES as a FIPS in February 1994.[113] Neither the encryption algorithm nor the key-splitting method was specified in the FIPS.[114] NIST's approval of EES followed a 1994 decision to approve an NSA-backed digital signature standard as a FIPS instead of the more popular digital-signature method already in use by industry. From the outside, it looked as if NIST was not listening to public input and was heading towards cryptographic standards that provided security but not necessarily privacy.[115] Few knew that NIST had actually pressed for the industry-favored technique but had been overruled in the joint TWG.[116] Then NIST announced its effort on AES.

NIST knew that for AES to be widely accepted, development of the new standard would require the participation of the cryptographic community,[117] but NSA's role in the standard's development was the elephant in the room.[118] What would happen if NSA submitted a candidate to

---

[112] "We received 320 comments, only 2 of which were supportive," reported F. Lynn McNulty, Associate Director for Computer Security at the National Institute of Standards and Technology. *Id*.

[113] FIPS PUBLICATION 185, *supra* note 108, at 2.

[114] *Id*. at 7–9.

[115] EES did not necessarily provide security. In 1994, Matt Blaze showed how to spoof the system so that a communication would be encrypted using EES but the keys would not be available to the U.S. government. Matt Blaze, *Protocol Failure in the Escrowed Encryption Standard*, PROC. OF THE 2D ACM CONF. ON COMPUT. COMMC'NS SEC. 59, 60 (1994), https://doi.org/10.1145/191177.191193 [https://perma.cc/H739-4HKW]. *See also* HAL ABELSON, ROSS ANDERSON, STEVEN M. BELLOVIN, JOSH BENALOH, MATT BLAZE, WHITFIELD DIFFIE, JOHN GILMORE, PETER G. NEUMANN, RONALD L. RIVEST, JEFFREY I. SCHILLER & BRUCE SCHNEIER, THE RISKS OF KEY RECOVERY, KEY ESCROW, AND TRUSTED THIRD PARTY ENCRYPTION 9–10 (1998), https://www.mattblaze.org/papers/escrowrisks98.pdf [https://perma.cc/2CSD-4TSY].

[116] Memorandum from Dennis K. Branstad & F. Lynn McNulty to John W. Lyons, Director of the Nat'l Inst. of Standards and Tech. (July 1990), *in* THIRD CPSR CRYPTOGRAPHY & PRIVACY CONFERENCE: SOURCEBOOK (David Banisar, Marc Rotenberg & Computer Professionals for Social Responsibility eds., 1993). FIPS 186 Digital Signature Standard (DSS) was published in 1994 but was replaced in 1998 by FIPS 186-1, which included the more popular RSA-based digital signature. NAT'L INST. OF STANDARDS & TECH., FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION 186-1: DIGITAL SIGNATURE STANDARD (DSS) 1, 6 (1998), https://csrc.nist.gov/CSRC/media/Publications/fips/186/1/archive/1998-12-15/documents/fips186-1.pdf [https://perma.cc/KPF9-RZGU] [hereinafter FIPS PUBLICATION 186-1].

[117] Smid, *supra* note 87, at 5–6.

[118] *Id*. at 9.

the competition?[119] Would anyone trust the new encryption standard if it turned out to be NSA's submission? And what if NSA informed NIST of a classified weakness in a different submission?[120] How could NIST deprecate a candidate without providing an explanation of the flaw?[121]

Neither issue came to pass.[122] NSA did not submit an algorithm. The public cryptographic community conducted cryptanalysis on the submitted algorithms, and none of the five finalists were believed to have security flaws. And the chosen algorithm, Rijndael, was considered sufficiently secure that several years later, NSA's trust in the chosen standard was demonstrated when the agency approved AES for protecting classified data so long as it was in an NSA-certified implementation.[123] But that takes us ahead of our story.

NIST's public competition to develop AES was a model of openness and transparency. The agency ran conferences in which there were public evaluations of the candidates;[124] the agency sought public comment through the Federal Register on the five finalists.[125] Candidate algorithms were evaluated according to security, cost, and algorithm and implementation characteristics (e.g., flexibility, algorithm suitability in hardware and software, and algorithm simplicity), with requirements discussed and considered in public.[126]

The cryptographic community, which early on in the selection process for AES had doubts about possible behind-the-scenes actions by NSA, was

---

[119] *Id*.
[120] *Id*.
[121] *Id*.
[122] Interview by Susan Landau with Brian Snow, Tech. Dir., Info. Assurance Directorate, Nat'l Sec. Agency (Dec. 27, 2012); Smid, *supra* note 87, at 9.
[123] NAT'L SEC. AGENCY, CNSS POLICY NO. 15, FACT SHEET NO. 1: NATIONAL POLICY ON THE USE OF THE ADVANCED ENCRYPTION STANDARD TO PROTECT NATIONAL SECURITY SYSTEMS AND NATIONAL SECURITY INFORMATION 2 (2003), https://csrc.nist.gov/csrc/media/projects/cryptographic-module-validation-program/documents/cnss15fs.pdf [https://perma.cc/65MX-2HMK].
[124] One candidate, submitted by Deutsche Telekom, was eliminated almost immediately after it was presented. *See* ELI BIHAM, ALEX BIRYUKOV, NIELS FERGUSON, LARS R. KNUDSON, BRUCE SCHNEIER & ADI SHAMIR, CRYPTANALYSIS OF MAGENTA 1 (1998), https://www.schneier.com/wp-content/uploads/2016/02/paper-magenta.pdf [https://perma.cc/A2SK-VWD7].
[125] Smid, *supra* note 87, at 13.
[126] James Nechvatal, Elaine Barker, Donna Dodson, Morris Dworkin, James Foti & Edward Roback, *Status Report on the First Round of the Development of the Advanced Encryption Standard*, 104 J. RSCH. NAT'L INST. STANDARDS & TECH. 435, 436 (1999), https://nvlpubs.nist.gov/nistpubs/jres/104/5/j45nec.pdf [https://perma.cc/JE79-8R38].

won over by NIST's transparency. AES was quickly adopted by numerous standards organizations, including ISO, IEEE 802.11[127] (Wi-Fi) for securing wireless networks, and the Internet Engineering Task Force (IETF)[128] for use in TLS.[129] AES was adopted in standards for transportation, the financial sector, media, ID cards, and much more.[130] NIST estimated that the benefit to the U.S. economy of AES was $250 billion.[131] This success was not just due to AES's use in communications protocols, but all uses of AES, including for such non-communications purposes as file encryption. The cooperative relationship that NIST had forged with the cryptographic research community during the AES competition led to the agency assuming a leadership role in the development of internationally adopted cryptographic standards.[132] The 2013 Snowden disclosure of a backdoor within Dual_EC_DRBG threatened to end that.

II. THE AFTERMATH OF DUAL_EC_DRBG

The backdoor that NSA inserted into Dual_EC_DRBG had consequences; it was not just a theoretical break, but an actual one. Bits generated by the algorithm were predictable by anyone who knew the secret information, revealing the keys and thus the encrypted information. In December 2013, *Reuters* reported that NSA had paid RSA Security $10 million to make Dual_EC_DRBG the default random-number generator in its

---

[127] The Institute of Electrical and Electronics Engineers (IEEE) develops standards in a number of industries; IEEE 802.11 is the working group that sets standards for wireless local area networks. *See IEEE 802.11™ Wireless Local Area Networks: The Working Group for WLAN Standards*, INST. OF ELECTRICAL & ELECTRONICS ENG'RS, https://www.ieee802.org/11 [https://perma.cc/4SL7-VM37] (last visited Jan. 17, 2022). Smid, *supra* note 87, at 14.

[128] The IETF develops many of the communications protocols used on the Internet. *See infra* Part III.B.2.

[129] Smid, *supra* note 87, at 14.

[130] David P. Leech, Stacey Ferris & John T. Scott, *The Economic Impacts of the Advanced Encryption Standard 1996–2017*, 3 ANNALS SCI. & TECH. POL'Y 142, 184 (2019), https://www.nist.gov/system/files/documents/2020/02/06/AES%202019.pdf [https://perma.cc/D7RF-YTA2].

[131] *Id.* at 222.

[132] This included the development of a secure hash function. *See* NAT'L INST. OF STANDARDS & TECH., FIPS PUBLICATION NO. 202, SHA-3 STANDARD: PERMUTATION-BASED HASH AND EXTENDABLE OUTPUT FUNCTIONS iii (2015), https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.202.pdf [https://perma.cc/D83V-4YD5].

BSAFE toolkit.[133] This opened the door to wider usage of the backdoored algorithm, including some implementations of SSL/TLS.[134]

It appears that NSA was not the only one to take advantage of the vulnerability built into Dual_EC_DRBG. Juniper, a U.S. company producing networking products, had used the Dual_EC_DRBG random-number generator in its operating system for their NetScreen VPN routers,[135] apparently at the behest of the Department of Defense.[136] According to Bloomberg, in 2012, a group linked to the Chinese government changed the parameters in the implementation of Dual_EC_DRBG in Juniper routers' operating system, creating a backdoor for an unknown party.[137] In other words, the vulnerability that NSA built into the NIST approved random-number generator was hacked by a third party, enabling a different actor—China—to listen to encrypted VPN communications.[138] In short, the worst that could happen—an approved encryption algorithm with a backdoor developed by a U.S. intelligence agency was hacked and used by an adversarial nation-state—had occurred.

NIST rectified the situation and remained a trusted provider of encryption standards used across Internet protocols. In Part II.A, we discuss

---

[133] Reuters reported that RSA Security's business personnel, not their technologists, made the decision to do so. Joseph Menn, *Exclusive: Secret Contract Tied NSA and Security Industry Pioneer*, REUTERS (Dec. 20, 2013), https://www.reuters.com/article/us-usa-security-rsa/exclusive-secret-contract-tied-nsa-and-security-industry-pioneer-idUSBRE9BJ1C220131220 [https://perma.cc/EE8C-MXDJ].

[134] As a result of other factors, the SSL backdoor was not always exploitable. *See* Stephen Checkoway, Matthew Fredrikson, Ruben Niederhagen, Adam Everspaugh, Matthew Green, Tanja Lange, Thomas Ristenpart, Daniel J. Bernstein, Jake Maskiewicz & Hovav Shacham, *On the Practical Exploitability of Dual EC in TLS Implementations*, *in* PROC. 23D USENIX SEC. SYMPOSIUM (2014), at 327, https://www.usenix.org/system/files/conference/usenixsecurity14/sec14-paper-checkoway.pdf [https://perma.cc/U2NX-DU64].

[135] Bob Worrall, *Important Juniper Security Announcement*, JUNIPER (Dec. 17, 2015), https://community.juniper.net/answers/blogs/dscholl1/2020/12/23/important-announcement-about-screenos [https://perma.cc/5E3L-7U65]; Kim Zetter, *Secret Code Found in Juniper's Firewalls Shows Risk of Government Backdoors*, WIRED (Dec. 18, 2015), https://www.wired.com/2015/12/juniper-networks-hidden-backdoors-show-the-risk-of-government-backdoors/ [https://perma.cc/SQT3-NX4X].

[136] Jordan Robertson, *Juniper Breach Mystery Starts to Clear with New Details on Hackers and U.S. Role*, BLOOMBERG (Sept. 2, 2021), https://www.bloomberg.com/news/features/2021-09-02/juniper-mystery-attacks-traced-to-pentagon-role-and-chinese-hackers [https://perma.cc/5G7V-BWZ5].

[137] This group was reported to be from APT 5, a hacking group affiliated with the Chinese government. *Id*.

[138] *Id*.

NIST's response to the Dual_EC_DRBG fiasco and, in Part II.B, the community's reaction.

A. NIST's Response to a Serious Failure

Within days of the *New York Times* article, NIST recommended against the use of Dual_EC_DRBG for random-number generation and reopened the standard for public comment,[139] a process that happens prior to FIPS approval. Seven months later, NIST removed its approval of Dual_EC_DRBG as a FIPS and urged vendors to replace implementations immediately if they had not already done so.[140] Though, for NIST, fixing a broken process that had allowed Dual_EC_DRBG to slip in as a standard was an even more critical issue. The concerns regarding Dual_EC_DRBG were not unknown prior to the September 2013 news story; questions were repeatedly raised about Dual_EC_DRBG's security prior to NIST's approval of the algorithm as a FIPS.[141] Yet, somehow, the standard was approved. As it removed the standard, NIST's Cryptographic Technology Group conducted an internal review to understand what allowed its standardization process to go so badly wrong.

The core of the problem was that despite previous conflicts between the two agencies over cryptographic standards in the 1990s, NIST did not anticipate that NSA would act as an adversary. NSA proposed a backdoored algorithm as a FIPS, claimed that the FIPS standardization was necessary for existing customers,[142] and then ensured wide deployment of the hacked system through the default implementation in the BSAFE toolkit. Not foreseeing such an action, NIST did not protect itself against the possibility.[143] During the FIPS approval process, NIST asked whether Dual_EC_DRBG *had been* corrupted but found no evidence of this; NIST

---

[139] NAT'L INST. OF STANDARDS & TECH., SUPPLEMENTAL ITL BULLETIN FOR SEPTEMBER 2013 (2013), https://csrc.nist.gov/CSRC/media/Publications/Shared/documents/itl-bulletin/itlbul2013-09-supplemental.pdf [https://perma.cc/2YY8-W4GG].

[140] *NIST Removes Cryptography Algorithm from Random Number Generation Recommendations*, NAT'L INST. OF STANDARDS AND TECH. (Apr. 21, 2014), https://www.nist.gov/news-events/news/2014/04/nist-removes-cryptography-algorithm-random-number-generator-recommendations [https://perma.cc/BPE2-HBQG].

[141] *See* Shumow, *supra* note 11; *see also* Gjøsteen, *supra* note 13.

[142] KELSEY, *supra* note 46, at 26.

[143] A researcher at NIST had asked questions about the generation of the parameters but was informed that "NSA had told not to talk about it." *Id*. at 23. That should have been a red flag, but the significance of this point was not noted at the time.

did not ask whether Dual_EC_DRBG *could have been* corrupted.[144] The latter question would have produced a different answer.

NIST's post-Snowden revisions to its cryptographic standard approval process needed to fix the loopholes that enabled such double dealing. In February 2014, the NIST's CSD released a draft document on its development process for cryptographic standards and guidelines in which it stressed that transparency, openness, balance, technical merits, and global acceptability guided its development of cryptographic standards.[145] To achieve balance, NIST would continue engaging with stakeholders in "*academia, industry*, and government" (emphasis added) during each stage of the process.[146] Clarifying that NSA did not govern NIST's actions, NIST explained that "NIST works closely with the NSA in the development of cryptographic standards…because of the NSA's vast expertise in cryptography" and because NIST was statutorily required under the Federal Information Security Management Act of 2002 to consult with NSA and other agencies on standards.[147]

Many concerns about the transparency of NSA's role in NIST cryptographic standards were raised during the public comment period for this draft document. Ian Goldberg, a leading cryptographer at the University of Waterloo, observed that, "[i]nformal channels are a way to breach transparency."[148] Naturally, much focus was on NSA; a group of U.S. civil-society organizations stated, "NIST should establish a policy wherein the Agency publicly explains the extent and nature of the NSA's consultation on future standards and any modifications thereto made at NSA's request."[149]

---

[144] *Id*. at 24–34.

[145] NAT'L INST. OF STANDARDS & TECH., NISTIR 7977, NIST CRYPTOGRAPHIC STANDARDS AND GUIDELINES DEVELOPMENT PROCESS (DRAFT) 1–2 (2014), https://csrc.nist.gov/csrc/media/publications/nistir/7977/final/documents/nistir_7977_draft.pdf [https://perma.cc/P35N-MXW4] [hereinafter NISTIR 7977 CRYPTOGRAPHIC STANDARDS].

[146] *Id*. at 3.

[147] *Id*. at 2.

[148] Ian Grigg, *Comments on NIST IR 7797, in* PUBLIC COMMENTS RECEIVED ON NISTIR 7797: NIST CRYPTOGRAPHIC STANDARDS AND GUIDELINES DEVELOPMENT PROCESS (DRAFT) 5 (Nat'l Inst. of Standards & Tech. ed., 2014), https://csrc.nist.gov/CSRC/media/Publications/nistir/7977/final/documents/public-comments-nistir7977.pdf [https://perma.cc/B5JB-KFRY] [hereinafter NISTIR 7797 PUBLIC COMMENTS].

[149] Access et al., *In the Matter of NIST Cryptographic Standards and Guidelines Development Process NIST IR 7977 (Draft), in* NISTIR 7797 PUBLIC COMMENTS, *supra* note 148, at 44. We noted that the statement, "NIST works closely with the NSA in the development of cryptography standards" needed clarification. "[Did] this mean that NSA

The Center for Democracy and Technology (CDT), a civil-society organization in Washington, D.C., focused on the need for proper documentation for "each feature of a cryptographic standard and the rationale behind choosing particularly critical parameters or features" as well as for proposed changes to an algorithm or parameters.[150] CDT also asked if NIST personnel are trained to spot potential cases of subversion of standards.[151] Respondents also had other issues, including intellectual property concerns. NIST's principles include seeking technologies unencumbered by patents; this issue was not directly relevant to the Dual_EC_DRBG situation.

Despite raising concerns about NIST's transparency, commenters pointed to the importance of NIST standards' international adoption. CDT recognized "the prominent role NIST cryptographic standards play in computing and networking contexts…[and that they are] widely adopted."[152] Kent Landfeld, the Director of Standards and Technology Policy at Intel subsidiary McAfee, further explained that "the result of NIST's work has become relevant worldwide, because industry has adopted NIST crypto standards as the best available."[153] Emblematic of many commenters. Microsoft Principal Software Development Engineer, Niels Ferguson, clarified that prior to those disclosures, "NIST has had international credibility to essentially set the cryptographic standards for the world."[154]

In spring 2014, NIST held an external review that included eminent cryptographers and computer security experts.[155] Echoing the comments made on NIST's draft document on developing cryptographic standards, this Committee of Visitors (CoVs) emphasized the "paramount importance" of

---

provides the algorithms (per DSA)? Does it mean that NSA vets the crypto algorithms (per the AES competition)? Does it mean that it promotes algorithms provided by NSA (per Dual EC-DRBG)?" Susan Landau, *Re: comments on NIST's Draft Cryptographic Standards and Guidelines Development* Process, *in* NISTIR 7797 PUBLIC COMMENTS, *supra* note 148, at 6.

[150] Ctr. for Democracy & Tech., *Comments on: Draft NIST Interagency Report 7797*, *in* NISTIR 7797 PUBLIC COMMENTS, *supra* note 148, at 32.

[151] *Id*.

[152] *Id*.

[153] Kent Landfield, *Re: Intel Comments in Response to INST IR 7977*, *in* NISTIR 7797 PUBLIC COMMENTS, *supra* note 148, at 38.

[154] Niels Ferguson, *Comments on Draft NIST Interagency Report 7977*, *in* NISTIR 7797 PUBLIC COMMENTS, *supra* note 148, at 35.

[155] NAT'L INST. OF STANDARDS & TECH., NIST CRYPTOGRAPHIC STANDARDS AND GUIDELINES DEVELOPMENT PROCESS: REPORT AND RECOMMENDATIONS OF THE VISITING COMMITTEE ON ADVANCED TECHNOLOGY OF THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY 1–2 (2014), https://www.nist.gov/system/files/documents/2017/05/09/VCAT-Report-on-NIST-Cryptographic-Standards-and-Guidelines-Process.pdf [https://perma.cc/R2ZM-XG6Q].

NIST having open and transparent processes for developing cryptographic standards.[156] It stressed that any processes during standardization should be documented.[157] The committee emphasized that it was critical for NIST's standardization process to have "the trust and support of the cryptographic community."[158]

One of the experts, Steve Lipner, at the time a Partner Director of Program Management at Microsoft, wrote that the set of principles guiding NIST's development of cryptographic standards, should be, "Security first ... Transparency of process ... Transparency of product."[159] Another expert, Professor Bart Preneel, a leading cryptographer and security expert,[160] wrote that the draft document on developing cryptographic standards should take the comments on the draft into account and that the document should "add 'due process' [while] 'avoiding undue influence.'"[161] Preneel urged that, in the context of NIST's work with NSA the words, "'consult,' 'coordination,' and 'work closely'" be clarified.[162] Cryptographer Ronald Rivest, the co-inventor of RSA, stated, "NIST's reliance on NSA expertise should be greatly reduced. All standards-related communications between NIST and the NSA

---

[156] *Id*. at 3.
[157] *Id*.
[158] *Id*.
[159] Steven B. Lipner, *Report of Steven B. Lipner to the NIST VCAT Subcommittee on Cybersecurity*, *in* NIST CRYPTOGRAPHIC STANDARDS AND GUIDELINES DEVELOPMENT PROCESS, *supra* note 155, at 5.
[160] Among his many efforts, Preneel ran NESSIE, the New European Schemes for Signatures, Integrity, and Encryption, a three-year E.U. program to design new encryption primitives, including block ciphers, hash functions, additive stream ciphers, and digital signatures. The three-year effort was organized much the way NIST cryptographic efforts since AES have been run, with open calls for submissions, workshops to evaluate the primitives, etc. *See* NEW EUROPEAN SCHEMES FOR SIGNATURES, INTEGRITY & ENCRYPTION, https://www.cosic.esat.kuleuven.be/nessie [https://perma.cc/JW7W-FN65] (last visited Dec. 21, 2021). In some sense, NESSIE was a European effort to match NIST's AES competition—it was to contribute to the AES standardization process—but its purpose was also European-centric, specifically to "maintain the strong position of European research while strengthening the position of European industry in cryptography." *New European Schemes for Signatures, Integrity, and Encryption*, EUR. COMMISSION, https://cordis.europa.eu/project/id/IST-1999-12324 (last updated Jun. 13, 2005) [https://perma.cc/768X-X6U6]. To the extent that the project contributed to the development of appropriate primitives, it was a success. But NESSIE made no dent in NIST's international leadership. NESSIE was a research project; it did not represent a strategic initiative to replace NIST's role with a European alternative.
[161] Bart Preneel, *Comments on the NIST Cryptographic Standards and Guidelines Development Program*, *in* NIST CRYPTOGRAPHIC STANDARDS AND GUIDELINES DEVELOPMENT PROCESS, *supra* note 155, at 15.
[162] *Id*. at 16.

should be in writing and part of the public record."[163]

NIST needed to wean itself from its dependency on NSA. Consulting with the intelligence agency was appropriate, but NIST needed the ability to "assess" and "reject" NSA's advice.[164] To do so, NIST needed to increase its own technical capabilities. And the relationship with NSA had to be clarified, with NIST senior management ensuring that changes were made that enabled NIST to function independently of NSA.[165]

NIST acted to bolster its technical expertise. From just four cryptographers on staff at the time of Dual_EC_DRBG's approval, by 2019, the number of cryptographers within NIST CSD had more than tripled.[166] In addition, the division hosts five to six guest researchers in cryptography annually, thus increasing its expertise as well as connections with academia.[167] Some guest researchers, sponsored by foreign governments, are from outside the U.S.[168] This bolsters international trust of NIST's cryptographic standards efforts.

In 2016, CSD publicly outlined its revised cryptographic standards and guidelines process to emphasize principles of transparency, openness, balance, integrity, technical merit, global acceptability, usability, continuous improvement, innovation, and intellectual property.[169] Opening with the transparency principle—"All interested and affected parties have access to essential information regarding standards and guidelines-related activities throughout the development process"[170]—demonstrated a clear break with

---

[163] Ronald Rivest, *Preliminary Findings Regarding NIST's Development of Cryptographic Materials*, *in* NIST CRYPTOGRAPHIC STANDARDS AND GUIDELINES DEVELOPMENT PROCESS, *supra* note 155.

[164] *See* NIST CRYPTOGRAPHIC STANDARDS AND GUIDELINES DEVELOPMENT PROCESS, *supra* note 155, at 4.

[165] *See id*.

[166] Interview with Lily Chen, Manager of Cryptographic Tech. Group, Comput. Sec. Div., Nat'l Inst. of Standards and Tech.; Donna Dodson, NIST Fellow, Chief Cybersecurity Advisor; John Kelsey, Computer Sci., Cryptographic Tech. Grp., Comput. Sec. Div., Nat'l Inst. of Standards and Tech.; Kerry McKay, Comput. Sc., Cryptographic Tech. Grp., Comput. Sec. Div., Nat'l Inst. of Standards and Tech.; Andrew Regenscheid, Comput. Sci., Cryptographic Tec. Grp., Comput. Sec. Div., Nat'l Inst. of Standards and Tech. (Mar. 19, 2018).

[167] *Id*.

[168] Personal communication from Lily Chen, Manager of Cryptography Tech. Group, Comput. Sec. Div., Nat'l Inst. of Standards and Tech., to authors (Mar. 26, 2021).

[169] NISTIR 7977 CRYPTOGRAPHIC STANDARDS, *supra* note 145, at 2–3.

[170] *Id*. at 2.

the situation that occurred with Dual_EC_DRBG. Continuous improvement explicitly articulated that "the cryptographic community [would be] encouraged to identify weaknesses, vulnerabilities, or other deficiencies in the algorithms specified in NIST publications."[171] NIST observed it needed to ensure its "internal capabilities [were] strong and effective, and that it [had] access to highly-capable external cryptographers."[172] The agency also committed to making every effort to ensure that contribution from *any* organization would "not compromise the security of any mechanism recommendation by NIST."[173]

Emphasizing its independence from NSA, NIST also implemented two critical changes to previous processes. First, submissions to proposed standards would be accepted only in writing, thus providing a paper trail of who suggested a change. Second, if NSA or any other agency assisted NIST in the development of new standards and guidelines, NIST would acknowledge that agency as the designer, even though NIST might not be able to list the actual individuals involved.[174] Noting that cryptographic competitions are an "especially powerful vehicle"[175] for developing particular cryptographic standards, a competition would have a single winner[176] and NIST would require winning submitters to agree to relinquish intellectual property rights.[177]

The agency sought to strengthen its ties to cryptographic standards organizations, which play a crucial role in adoption of strong cryptography standards globally.[178] NIST publicly committed to acting as a standards organization intent on putting strong cryptographic standards for worldwide use—and not as an arm of the U.S. government undermining such efforts.

While these changes were intended to restore trust, there was no guarantee that the cryptographic research community would respond

---

[171] *Id.* at 3.
[172] *Id.* at 1.
[173] *Id.* at 2.
[174] *Id.* at 10 n.2 ("The names of some NSA staff cannot, by law, be publicly revealed. 50 U.S.C. §402 note. Freedom of Information Act requests for documents involving any NIST-NSA collaboration are normally reviewed by both organizations and exempted or excluded information, which may include the names of specific NSA participants as noted, may be redacted.").
[175] *Id.* at 13.
[176] *Id.* at 19.
[177] *Id.* at 18.
[178] *Id.* at 11.

favorably to NIST's commitments. Without community support, NIST would not have been able to move past the Dual_EC_DRBG situation.

B. The Cryptographers' Response

As we noted earlier, the Dual_EC_DRBG situation played out against the backdrop of a four-decade conflict over U.S. encryption policy and over a decade of cooperation and respect between NIST and the international cryptographic research community. Both aspects—the four-decade history of conflict with the U.S. government and the decade-and-a-half of a healthy working relationship with NIST—were exhibited in the cryptographers' response to NIST.[179] Not surprisingly, they initially distrusted NIST.[180]

Many cryptographers held doubts for years about Dual_EC_DRBG. Among those were D.J. Bernstein, a computer science professor at the University of Illinois at Chicago, and Tanja Lange, a professor of cryptography at Eindhoven University of Technology.[181] Bernstein was something of a folk hero in the cryptography community for taking on the U.S. government in the 1990s over the publication and export of cryptographic algorithms—and winning.[182]

Only months before the Snowden disclosure, Bernstein and Lange presented work on the security risks of the NIST elliptic curves, including

---

[179] The U.S. government is not a monolith, and different agencies held different points of view on the encryption issue. The four-decade conflict was originally between the private sector and NSA; it later expanded to include the FBI. Since the change in export controls in 2000, the FBI has argued strongly for controls on encryption; at least in public, NSA has not.

[180] *See, e.g.*, Kim Zetter, *How a Crypto "Backdoor" Pitted the Tech World Against NSA*, WIRED (Sept. 24, 2013), https://www.wired.com/2013/09/nsa-backdoor/ [https://perma.cc/3VQR-FKC8] (describing NIST as facing "a crisis of confidence"); Matthew Green, *On the NSA*, A FEW THOUGHTS ON CRYPTOGRAPHIC ENG'G (Sept. 6, 2013), https://blog.cryptographyengineering.com/2013/09/06/on-nsa [https://perma.cc/5LBW-FND5] (suggesting that cryptographers would have to "re-evaluate" their relationship with NIST).

[181] Both provided comments on the NIST draft document on developing cryptographic standards. *See* Daniel J. Bernstein, *Comments on nistir_7977_draft.pdf*, *in* NISTIR 7797 PUBLIC COMMENTS, *supra* note 148, at 16
(criticizing the "reckless pace" of NIST cryptographic standardization efforts); Tanja Lange, *Comments on NISTIR 7977*, *in* NISTIR 7797 PUBLIC COMMENTS, *supra* note 148, at 48–51 (focusing on concerns about transparency and openness).

[182] Bernstein won in the Appeals Court; the U.S. government declined to take the case to the Supreme Court. The issue was whether publication of cryptographic code on a webpage constituted violation of export controls. *See* Bernstein v. U.S. Dep't of Just., 176 F. 3d 1132, 1141 (9th Cir.), *reh'g granted, withdrawn*, 192 F. 3d 1308 (9th Cir. 1999).

Dual_EC_DRBG.[183] NIST's efforts did not impress Bernstein, who objected to the speed at which NIST was issuing standards—he felt there was a lack of time to properly vet the standards—and did not trust that there was not a backchannel between NIST and NSA.[184] But Bernstein was largely an outlier in his distrust of NIST.

As NIST was working through the changes in the standardization process to prevent future Dual_EC_DRBGs, the agency was also simultaneously mounting new cryptographic competitions. In 2015, NIST declared its intent to develop standards for post-quantum cryptography.[185] NSA had publicly signaled that a transition was important, though it was unclear whether it was quantum computing or weaknesses in current public-key standards that triggered the agency's concern.[186] For the effort to succeed, the participation of the world's leading cryptographers was crucial.

NIST announced a 2015 workshop to explore the problem—and the cryptographers came.[187] Cryptographic experts from all over the world

---

[183] *See* Daniel J. Bernstein & Tanja Lange, *Security Dangers of the NIST Curves*, INT'L STATE OF THE ART CRYPTOGRAPHY WORKSHOP (May 31, 2013), https://cr.yp.to/talks/2013.05.31/slides-dan+tanja-20130531-4x3.pdf [https://perma.cc/9XRD-J5D9].

[184] *See* Daniel J. Bernstein, *NIST's Cryptographic Standardization Process*, CR.YP.TO BLOG (Apr. 11, 2014), https://blog.cr.yp.to/20140411-nist.html [https://perma.cc/YE2R-PYJ9].

[185] *Workshop on Cybersecurity in a Post-Quantum World*, NAT'L INST. OF STANDARDS & TECH. (Mar. 26, 2014), https://www.nist.gov/news-events/events/2015/04/workshop-cybersecurity-post-quantum-world [https://perma.cc/JTY8-H2Q9].

[186] In 2005, NSA released a set of algorithms, Suite B, that included AES, Elliptic-Curve Diffie Hellman, Elliptic-Curve Digital-Signature Algorithm, and Secure Hash Algorithm, which could be used to secure a communications network. *See Suite B Cryptography*, NAT'L SEC. AGENCY (Jan. 15, 2009), http://archive.today/mFaN [https://perma.cc/7P3Q-JVPU]. But, in 2015, the NSA issued a somewhat peculiar statement: "For those partners and vendors that have not yet made the transition to Suite B elliptic curve algorithms, we recommend not making a significant expenditure to do so at this point but instead to prepare for the upcoming quantum resistant algorithm transition. . . . Unfortunately, the growth of elliptic curve use has bumped up against the fact of continued progress in the research on quantum computing, which has made it clear that elliptic curve cryptography is not the long term solution many once hoped it would be. Thus, we have been obligated to update our strategy." *Commercial National Security Algorithm Suite*, NAT'L SEC. AGENCY (Aug. 19, 2015), https://apps.nsa.gov/iaarchive/programs/iad-initiatives/cnsa-suite.cfm [https://perma.cc/9MZZ-XHSP]; *see also* Koblitz & Menezes, *supra* note 10, at 8.

[187] *See Workshop on Cybersecurity in a Post-Quantum World: Accepted Papers*, NAT'L INST. OF STANDARDS & TECH., https://csrc.nist.gov/csrc/media/events/workshop-on-cybersecurity-in-a-post-quantum-world/documents/accepted-papers-postquantum.pdf [https://perma.cc/VEZ9-EVPA]. NIST approached the standardization of post-quantum cryptography in a very deliberate manner, taking into account the many unknown unknowns. The agency's timeline was slow and deliberate, with a plan to release draft criteria in 2016,

attended. While not everyone who participated agreed that NIST was trustworthy, the presence of so many leading cryptographers was a good sign. So were the number and quality of submissions (eighty-two submissions from residents of twenty-five countries and six continents).[188]

Despite the importance of its post-quantum cryptographic standardization effort, NIST did not call the process a "competition," which would trigger certain requirements under its cryptographic standards developments process.[189] Developing standards for post-quantum cryptography is fraught with uncertainty; thus, the commitments that NIST had previously laid out for how competitions were not a good fit for post-quantum standards development.[190]

The best solution in terms of security for post-quantum cryptography is to pick "good choices" in various categories of algorithms.[191] Rather than pick a "winner"[192]—part of the process for a competition[193]—NIST sought the option of standardizing several submissions, eliminating others, and potentially leaving some for further study.[194] In fact, in 2020, NIST did exactly that with a decision to go onto a fourth round of evaluations.[195] But

---

select at least one algorithm for each of the different functionalities needed (digital signature, encryption, and key exchange), and allow three to five years of public vetting before standardizing. *See* LILY CHEN, STEPHEN JORDAN, YI-KAI LIU, DUSTIN MOODY, RENE PERALTA, RAY PERLNER & DANIEL SMITH-TONE, NISTIR 8105: REPORT ON POST-QUANTUM CRYPTOGRAPHY 7 (2016).

[188] DUSTIN MOODY, NAT'L INST. OF STANDARDS & TECH., THE SHIP HAS SAILED: THE NIST POST-QUANTUM CRYPTO COMPETITION 33, 35 (2017), https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/asiacrypt-2017-moody-pqc.pdf [https://perma.cc/C356-JC66].

[189] NISTIR 7977 CRYPTOGRAPHIC STANDARDS, *supra* note 145, AT 16–19.

[190] Another distinction is that, unlike a competition, there was no requirement that the standardized algorithms give up intellectual property rights.

[191] MOODY, *supra* note 188, at 36.

[192] NIST's announcement states that the agency will standardize "one *or more* quantum-resistant public-key cryptographic algorithms" (emphasis added); *see Post-Quantum Cryptography (PQC)*, NAT'L INST. OF STANDARDS & TECH, https://csrc.nist.gov/projects/post-quantum-cryptography/ [https://perma.cc/D48P-J7F7] (last visited Jan. 16, 2022).

[193] NISTIR 7977 CRYPTOGRAPHIC STANDARDS, *supra* note 145, at 19.

[194] *Is the NIST PQC Standardization Process a Competition? (Old Q7) Post-Quantum Cryptography FAQS*, NAT'L INST. OF STANDARDS & TECH. (2021), https://csrc.nist.gov/Projects/post-quantum-cryptography/faqs [https://perma.cc/7UVC-N7XQ].

[195] *PQC Standardization Process: Third Round Candidate Announcement*, NAT'L INST. OF STANDARDS & TECH. (July 22, 2020), https://www.nist.gov/news-events/news/2020/07/pqc-standardization-process-third-round-candidate-announcement [https://perma.cc/TW6K-A82M].

even though NIST did not call its standardization process a competition, cryptographers did. And so over time, NIST did, too—although only in quotes.[196]

Why were cryptographers willing to participate in a post-quantum cryptography effort on the heels of Dual_EC_DRBG? First, the situation was not nearly as black and white as it might seem in a newspaper headline. In dealing with NSA, and especially at a time when its own technical resources were quite limited, NIST was operating in a very complex situation. The aftermath of the Dual_EC_DRBG situation—more resources and technical personnel for the Cryptographic Technology Group, stricter and more transparent rules for handling communications with NSA, and explicit and strong backup from NIST leadership—led Professor Bart Preneel, who had served on the CoV, to conclude that post-Dual_EC_DRBG NIST is "doing a good job, doing the best [it can] in a difficult situation."[197]

Many computer scientists also had a long history with NIST in the security space; that experience tempered their criticism of NIST. Steve Lipner,[198] a long-time leader in computer security who also served for many years on a federal board advising on U.S. computer security and privacy[199]—and thus had seen many of NIST's activities in that space—viewed the Dual_EC_DRBG situation as something "that happened" to NIST, rather than

---

[196] DUSTIN MOODY, NAT'L INST. OF STANDARDS AND TECH., ROUND 2 OF THE NIST PQC COMPETITION: WHAT WAS NIST THINKING? (2019), https://csrc.nist.gov/CSRC/media/Presentations/Round-2-of-the-NIST-PQC-Competition-What-was-NIST/images-media/pqcrypto-may2019-moody.pdf [https://perma.cc/2HQR-FEF2].

[197] Interview with Bart Preneel, Professor, Katholieke Universiteit Leuven in Belgium (Apr. 18, 2019).

[198] Lipner is an expert in software security and vulnerabilities, Internet security, and organizational change for security. He founded and led the development of the Security Development Lifecycle team that significantly improved the security of Microsoft's software. *Future of Encryption*, NAT'L ACAD. OF SCIS., ENG'G & MED., https://www.nationalacademies.org/our-work/future-of-encryption#sectionProjectScope [https://perma.cc/J9W2-4GCP] (last visited Feb. 7, 2022).

[199] The Computer Science Security and Privacy Advisory Board was set up in 1989 by the 1987 *Computer Security Act*, P.L. 100-235 § 21. Its role was to advise the Secretary of Commerce and the Director of the National Bureau of Standards on security and privacy issues of federal computer systems. The Board's name and role were changed as a result of Title III of *the E-Government Act of 2002*, P.L. 107-347. § 304 changed the board's name to the Information Security and Privacy Advisory Board, and added the review of proposed standards and guidelines to its role. The board is also now required to advise the Director of the Office of Management and Budget. Lipner has served three terms on the board: 1989–93, 2000–06, and 2018–present; he has been Chair of the board since early 2019.

something NIST caused.[200] From his years of experience working in security in industry, Lipner noted that "[a] lot of good will [is] directed at NIST."[201]

And it was not just good will. NIST delivered value, and that made its cryptographic competitions attractive. One eminent cryptographer, when asked, "Why trust NIST?," explained that the value of NIST's work comes from the fact that many cryptographers from around the world participate in the NIST standardization efforts and work to evaluate an algorithm's security. Then there is the impact of being picked as a FIPS. "If NIST chooses my algorithm," the cryptographer said, "[t]hen my algorithm is used all over the world."[202]

So while NIST was not the only organization running post-quantum cryptography efforts,[203] it was the only organization running an international standardization effort that consistently brought the best minds to work on a problem. It was able to do this because it is the only organization with sufficient capacity to do so.

III. WHY THIS RESOLUTION?

In the wake of the Snowden disclosures regarding Dual_EC_DRBG, NIST made the right moves to restore its reputation. But two other factors contributed to NIST's ability to continue as a provider of internationally accepted cryptographic standards. First, NIST was able to marshal organizational and technical resources to develop internationally trusted cryptographic standards; as a result, NIST provides organizational and technological "capacity" to develop cryptographic standards. Second, currently no other body is in a position to do the same. In Part III.A, we examine NIST's strengths in the role of provider of cryptographic standards, using that to study in Part III.B which, if any, alternative players might have been able to step in.

---

[200] Interview with Steve Lipner, Chairman of the Information Security and Privacy Advisory Board (Mar. 12, 2019).
[201] *Id.*
[202] Interview with anonymous senior cryptographer from Asia (Feb. 4, 2020).
[203] Walter Fumy, Frank Morgner & Andreas Hülsing, *PQCRYPTO: Post-Quantum Cryptography for Long-Term Security, D 5.2 Standardization: Final Report* §3 (2018).

A. Understanding the Capabilities NIST Brings to Cryptography Standardization

NIST's immediate response to the Dual_EC_DRBG situation—combined with the thoroughness of its investigation, its improved process transparency, and its inclusiveness—did much to reinstate its reputation as a trustworthy agency. Specifically, these factors ensured fairness.[204] Adam Langley, a Google software engineer managing the low-level cryptography library that supports many of the company's products, observed that NIST's legacy of running high-quality competitions with multiple competition rounds conducted in a public and transparent manner creates community trust.[205] Moreover, since NIST's inclusive process draws in both industry and academic responses, NIST's reservoir of goodwill, built within the research community, especially with the AES competition, also helped reestablish trust after the Dual_EC_DRBG situation.[206] Lastly, the agency's non-regulatory nature simplified NIST's relationship with industry representatives, encouraging participation.[207]

The other aspect that aided NIST's recovery was the agency's organizational and technical capacity to develop civil-sector cryptographic standards, a capacity that appears unique among voluntary standards organizations. NIST's organizational capacity was established on paper by the *Brooks Act of 1965*, authorizing NIST as the provider of automatic data-processing standards. As the developer of FIPS, NIST was in a powerful role. The private sector often adopts FIPS used in federal computing systems.[208]

As policy scholars Douglas and Janet Vinzant have written, organizational capacity requires more than establishing capacity on paper. Capacity includes organizational autonomy, which the Brooks Act of 1965 did not fully provide, but the Computer Security Act of 1987 did. Capacity also requires structural support for planning and resource allocation processes. In its early years, NIST's role in developing FIPS was not matched by structural support. The Brooks Act did not provide resources.[209] Indeed, when NIST was tasked with soliciting proposals for a cryptographic

---

[204] TIM BÜTHE & WALTER MATTLI, THE NEW GLOBAL RULERS 215–26 (2011).
[205] Interview with Adam Langley, Software Engineer, Google (June 14, 2019).
[206] *Id*.
[207] *Id*.
[208] NAT'L INST. OF STANDARDS & TECH., *FIPS General Information*, https://www.nist.gov/itl/fips-general-information [https://perma.cc/5N7W-XLS4] (last visited Dec. 20, 2021).
[209] Brooks Automatic Data Processing Act, Pub. L. No. 89-306, 79 Stat. 1127 (1965).

algorithm to secure sensitive data held by non-national security federal agencies, it had to rely heavily on NSA during DES's development.[210]

The Vinzants also point to external stimuli in the form of threats and opportunities that might motivate an organization to evolve and increase its capacity. In large part, NIST's external threat came from NSA, which sought—and often succeeded—in controlling NIST's cryptographic standards work.[211] The opportunity, which was not realized in the first decade after the passage of the Computer Security Act of 1987, was that by law, NIST had the role of developer of non-national security standards.[212]

The passage of the Act improved NIST's organizational capacity, but the 1989 Memorandum of Understanding between the Department of Commerce and the Department of Defense[213] regarding implementation of the Act gave critical control over aspects of cryptographic standard development to NSA,[214] undermining aspects of the Act. This prevented NIST from taking advantage of the opportunities provided by the Act. Decisions about FIPS often went the way NSA wanted rather than the direction that NIST technologists thought appropriate.[215]

When the Act was passed in 1987, the public Internet was not a reality—nor did legislators or NIST necessarily even imagine it. But by the mid-1990s, industry and NIST alike could see what was on the horizon. NIST knew it was time to replace DES, which was becoming increasingly insecure.[216] Although there were private-sector alternatives to DES, these did not interoperate.[217] This situation created complexity; NIST hoped that it could develop a DES replacement that would be adopted by the government and the commercial sector.[218]

---

[210] DAVID P. LEECH & MICHAEL W. CHINWORTH, NAT'L INST. OF STANDARDS & TECH., THE ECONOMIC IMPACT OF NIST'S DATA ENCRYPTION STANDARD (DES) PROGRAM (PLANNING REPORT 01-02, 2001) 12 (2001), https://www.nist.gov/system/files/documents/2017/05/09/report01-2.pdf [https://perma.cc/TZ74-YTTY].

[211] See *supra* Part I.C–D.

[212] Computer Security Act of 1987, Pub. L. 100-235, § 278g-3, 101 Stat. 1724, 1724–27 (1987) (repealed 2002).

[213] 1989 NIST-NSA Memorandum of Understanding, *supra* note 74, at 2.

[214] *See* discussion of the Technical Working Group *supra* § II.C.

[215] Landau, *supra* note 80, at 421–22.

[216] Smid, *supra* note 87, at 4–5.

[217] Leech, Ferris & Scott, *supra* note 130, at 160.

[218] Smid, *supra* note 87, at 5.

With the changing needs for encryption that the Internet brought, organizational autonomy and external stimuli that the Vinzants described became aligned. So did the internal factors. NIST management saw that the negative response to the digital signature standard and EES (Clipper) was hindering acceptance of these technologies. The commercialization of the Internet in the late 1990s created incentives to secure online transactions and communications, providing increased opportunity for NIST to develop internationally trusted cryptographic standards that would secure Internet communications protocols.

At that time, there were two fundamental problems with the NIST efforts: a technological one, in which the private sector was unwilling to accept the technologies due to it being unsuitable for their needs;[219] and an organizational one, that NIST had approached the approval of a new FIPS as an essentially government affair. The latter approach might have worked in the 1970s, when the federal government was a prime, if not the prime, user of cryptographic standards. But this approach would not succeed in the brave new world of mass private sector use of cryptographic systems. The government could not work alone to develop and approve FIPS that it hoped would have wide commercial use. A new approach was needed to do so.[220]

NIST faced another problem as well: developing an advanced encryption standard to replace DES would require technical expertise beyond NIST's capacity in the mid-1990s. Additionally, the public outcry over Clipper meant that if an advanced standard were to be accepted, it needed buy-in from the cryptographic research community.[221]

NIST successfully threaded the needle. As we described in Part I.C, NIST developed a plan to fully involve the cryptographic research community from the start of the standard's development process.[222] In this way, NIST used its organizational capacity to ensure technical capacity.

NIST organized the development of the AES competition to attract academic participants who formed the heart of the international cryptographic research community. The agency ran three conferences for

---

[219] Some industries saw no problem with a key-escrow approach to encryption—but did find a problem with one in which the keys were stored with agencies of the U.S. government.
[220] Smid, *supra* note 87, at 4–5.
[221] *Id.*
[222] *Id.*

introducing, examining, and vetting the submissions.[223] Organized like academic cryptography conferences, the first meeting consisted of presentations of the submitted algorithms; the second analyzed these submissions based on security, (software) efficiency, and flexibility; and the third considered efficiency in hardware.[224] Participants utilized technical expertise to vet AES proposals, and in some cases eliminated submissions quickly.[225] Meanwhile, NIST deployed its technical expertise in various ways, including measuring efficiency of software implementations.[226]

A half-decade after the AES effort, NIST ran the SHA-3 competition to determine a new hash standard. Hash functions provide a way of ensuring the integrity of digital data (e.g., that the file you receive has not been tampered with) and are what Ralph Merkle, a c-inventor of public-key cryptography, has called the "duct tape" of cryptography.[227] In 2004, Xiaoyun Wang demonstrated an attack against NIST's secure hash function,[228] prompting NIST to launch a competition for a replacement.[229] The SHA-3 competition, run much the way the AES competition had been done, received similar plaudits.[230]

NIST acquired resources to run cryptographic competitions, community outreach, and sponsorship of various meetings. This infrastructure support was critical to the project's success. According to Kenny Paterson, an eminent cryptographer who served as co-chair of the

---

[223] To attract the academics, the meetings were held in conjunction with other conferences (CRYPTO in 1998, Fast Software Encryption in 1999 and 2000). *Id.* at 6.

[224] *Id.* at 11.

[225] *See* BIHAM ET AL., *supra* note 124 and accompanying text.

[226] Smid, *supra* note 87, at 10–11.

[227] Peter Gutmann, David Naccache & Charles C. Palmer, *When Hashes Collide*, 3 IEEE SEC. & PRIVACY 68, 68 (2005).

[228] Wang's work was presented at the CRYPTO 2004 "rump" session. Xiaoyun Wang, Dengguo Feng, Xuejia Lai, & Hongbo Yu, *Collisions for Hash Functions MD4, MD5, HAVAL-128, and RIPEMD*, https://eprint.iacr.org/2004/199 (Aug. 17, 2004). This was followed by even stronger forms of attack by Wang and others the following year. This research precipitated the withdrawal of approval for SHA and the development of new hash standards.

[229] Announcing Request for Candidate Algorithm Nominations for a New Cryptographic Hash Algorithm (SHA-3) Family, 72 Fed. Reg. 62,212–20 (Nov. 2, 2007).

[230] *See, e.g.*, Bart Preneel, *in* NIST CRYPTOGRAPHIC STANDARDS AND GUIDELINES DEVELOPMENT PROCESS, *supra* note 155, at 57; Bruce Schneier, *Keccak is SHA-3*, SCHNEIER ON SECURITY (Oct. 2, 2012), https://www.schneier.com/blog/archives/2012/10/keccak_is_sha-3.html [https://perma.cc/D2BA-T7EQ].

Internet Research Task Force's (IRTF)[231] research group on cryptography,[232] only a few actors, such as large U.S. companies, could match NIST's resources for these public activities.[233] Such resources are crucial for the standards development process. These other actors lack NIST's ability to approve a proposed algorithm as a FIPS. Without this mandate, these actors are missing an important aspect of organizational capacity—though as we discuss later, occasionally they have played such a role.

NIST's technical capacity also played an important role in the establishment of its legitimacy. Cryptographic algorithms are complex mathematical functions in which a seemingly minimal change in design can render a secure technique insecure. Thus, much technical expertise is needed to evaluate proposed cryptographic systems. NIST relies on this outside expertise for standards development and evaluation, and uses its own, relatively small staff to cultivate informal networks of cryptographers. The NIST competitions demonstrate how this takes place.

To bring in external technological expertise, NIST starts a standardization effort through open online and offline dialogues about the need and requirements for a new algorithm.[234] Then, NIST posts an announcement in the Federal Register describing "the submission requirements, schedule and selection criteria" for the new algorithm.[235] For each round of the competition, NIST holds a major cryptographic research conference. Following each round, it announces a few selected criteria until it selects the winner. With each round, NIST also releases a report that explains its selection rationale.[236] Once NIST selects a single algorithm,[237] the agency writes a final report and "formally propose[s] a standard or guideline for the algorithm through the normal FIPS or Special Publication

---

[231] The IRTF, which works in parallel with the IETF, examines longer term research issues related to the Internet protocols; it is divided into research groups, of which the Crypto Forum Research Group is one; *see Internet Research Task Force*, INTERNET RSCH. TASK FORCE, https://irtf.org [https://perma.cc/T9P2-7G9F].

[232] *Crypto Forum*, DATATRACKER, https://datatracker.ietf.org/rg/cfrg/about [https://perma.cc/2LHC-278G] (last visited Mar. 5, 2022). The group advises the IETF on the security of cryptographic protocols. *Id.*

[233] Interview with Kenny Paterson, then Professor of Information Security at University of London (June 13, 2019). Paterson is now a Professor of Computer Science at Eidgenössische Technische Hochschule Zürich.

[234] NISTIR 7977 CRYPTOGRAPHIC STANDARDS, *supra* note 145.

[235] *Id.*

[236] *Id.*

[237] In the case of post-quantum cryptography, it is likely to be several algorithms; *see supra* Part II.B.

process."[238] Most importantly, NIST welcomes public comments at each stage of the process.[239] As this description makes it clear, the NIST staff run open, transparent, and inclusive standardization efforts among cryptographers who contribute their technical expertise to the standard's development.

Even though NIST had almost no cryptographic expertise of its own throughout the 1970s to the 1990s, NIST greatly improved its cryptographic capabilities beginning in the 2000s and then speeding up after the Dual_EC_DRBG debacle. Although some noted that while the agency will not design proposed standards and will never be in a position to compete with NSA's cryptographic capabilities,[240] there was strong agreement that CSD is in a healthy position to run a cryptographic standards competition.[241]

NIST's position relative to NSA strengthened in 2010 with an updated MOU between the two agencies. It explicitly stated that the Department of Commerce is

> authorized to exercise its functions for . . . international organizations of which the United States is a member, for governments of friendly nations, . . . or for any scientific society, educational institution, firm, corporation, or individual within the United States or friendly countries engaged in manufacturing or other pursuits requiring the use of standards or standard measuring instruments.[242]

In another change—and in recognition of NIST's capabilities—the MOU declared that NSA was to rely on NIST guidelines and standards as long as they were consistent with national security needs.[243] This was, perhaps, in

---

[238] NISTIR 7977 Cryptographic Standards, *supra* note 145.

[239] Here is an example of such public comments received on NISTIR 7977: NISTIR 7797 PUBLIC COMMENTS, *supra* note 148.

[240] Interview with Adam Langley (June 14, 2019).

[241] *See, e.g.*, *supra* Part II.B.

[242] The exercise of these functions must be in coordination with other agencies of the U.S. government. Memorandum of Understanding Between the Director of the National Institute of Standards and Technology (NIST) and the Director of the National Security Agency (NSA) Concerning the Implementation of the Federal Information Security Act of 2002, ¶ E (2010), https://csrc.nist.gov/CSRC/media/Projects/Crypto-Standards-Development-Process/documents/NIST_NSA_MOU-2010.pdf [https://perma.cc/3TN4-KRH5] [hereinafter 2010 NIST-NSA Memorandum of Understanding].

[243] "NSA shall 'draw upon information security and other cyber security technical guidelines and standards developed by NIST for non-national security systems so the extent that the

recognition that AES had proved useful for protecting classified information.[244] NSA was also to consult with NIST on the research and development related to various types of security technologies.[245] This was a far cry from the imbalance that existed in the 1989 MOU, which in practice made NIST subservient to NSA.

B. Lack of Alternative Actors to Lead International Civil-Sector Cryptography

NIST's effort to recover from the Dual_EC_DRBG was rewarded. To a certain degree, this was because NIST quickly applied fixes, preventing similar situations from reoccurring in the future. NIST was able to do this in part because it has capabilities that cannot be matched by other institutions.

NIST's unique organizational capacity for developing new cryptographic standards comes from law, including NIST's responsibility for developing FIPS, and from policy, including support from the government. Moreover, NIST's organizational capacity is strengthened by the increasing importance of strong cryptography to U.S. national and economic security. The agency's role as a non-national-security government agency responsible for developing non-national-security cryptography standards is unusual. No other nation has a federal agency involved in such activities; while the E.U. has periodically funded research in cryptographic standards, these programs are of short duration and do not carry with them any mandate for implementation. The fact that the FIPS cryptographic standards are often mandatory for non-national-security federal agencies[246] provides a natural market for the standards—and thus can help seed the standard in the private sector. This gives NIST organizational capacity that is typically not enjoyed by other standards organizations. Meanwhile, NIST's technical capacity comes largely from a combination of NIST's own capabilities and, critically, from the cryptographic research community, which the agency now works hard to engage in FIPS endeavors.

NSA determines that such guidelines are consistent with the requirements for protecting national security systems in the information that resides they are in.'" *Id.*

[244] NATIONAL POLICY ON THE USE OF THE ADVANCED ENCRYPTION STANDARD, *supra* note 123.

[245] Those listed were "trusted technology, security automation techniques, and personal identification methods." 2010 NIST-NSA Memorandum of Understanding, *supra* note 242, at 2.

[246] *Compliance FAQs: Federal Information Processing Standards*, NAT'L INST. OF STANDARDS & TECH. (Nov. 15, 2019), https://www.nist.gov/standardsgov/compliance-faqs-federal-information-processing-standards-fips [https://perma.cc/7SU6-ST2F].

The role in developing FIPS and U.S. government support are advantages that put NIST in a unique position with respect to other organizations developing cryptographic standards. This does not mean that other organizations might not assume the role, in whole or in part, in the future, but NIST's position has held over the last two decades.

Competition falls into two categories: nations, or groups of nations, and standards organizations. National competitors themselves fall into essentially two categories: the first being China and Russia, the second, the European Union. Both China and Russia have strong expertise in cryptography. In 2004, a Chinese researcher, Xiaoyun Wang, produced the first attack against the NIST secure hash function,[247] and Russian cryptography work has long been held in high regard.[248] But both nations use their legal systems to facilitate state surveillance that does not operate under rule of law.[249] This has created international distrust in cryptographic standards developed by the Chinese and Russian national agencies, making the community unwilling to adopt these standards.

By contrast, various smaller nations, including many in Europe as well as Japan and South Korea, have technical capacity. Indeed, European applied cryptography research, the type of work that leads to standards, is more extensive and stronger than U.S. work in this area—but Europe, Japan, and South Korea have chosen not to engage in cryptographic standards efforts. In part, this is because these nations lack a large national audience for a national standard.

Consider, for example, the case of Japan. In 2000, Japan set up a Cryptography Research and Evaluation Committee (CRYPTREC) to recommend cryptographic systems for use by non-national-security agencies in Japan; its advisory board includes academics and members of the government and industry.[250] It has not been very successful. Its set of recommendations includes some Japanese ciphers. One, Camellia, has been

---

[247] *See* WANG, *supra* note 228.

[248] KAHN, *supra* note 22, at 670–71.

[249] *See generally* HUMAN RIGHTS WATCH, CHINA'S GLOBAL THREAT TO HUMAN RIGHTS (2020), https://www.hrw.org/world-report/2020/country-chapters/global# [https://perma.cc/VT2H-RALT]; KAI STRITTMATTER, WE HAVE BEEN HARMONIZED: LIFE IN CHINA'S SURVEILLANCE STATE (2020); ANDREI SOLDATOV & IRINA BOROGAN, THE RED WEB: THE STRUGGLE BETWEEN RUSSIA'S DIGITAL DICTATORS AND THE NEW ONLINE REVOLUTIONARIES (2015).

[250] *See generally About CRYPTREC*, CRYPTREC, https://www.cryptrec.go.jp/en/about.html [https://www.cryptrec.go.jp/en/about.html] (last visited Feb. 28, 2022).

included in various open-source libraries (and was for a time, used for TLS), but adoption outside Japan is limited.[251] It seems that only Japanese companies regard CRYPTREC as being better than NIST.

Some might argue that Israel could be another possible candidate given that Israeli cryptographers rank among the best in the world.[252] Yet Israel is not seen as a trusted party for developing cryptographic standards; it does not employ the same civil liberties protections as most liberal democracies, and the recent disclosures about NSO spying have increased distrust.[253] Given these two factors, other nations are loathe to trust Israel to develop secure cryptography standards for fear that these might include a subtle hidden backdoor.[254]

It is also unlikely that industry can play a central role as the long-term developer of widely used cryptographic standards—which is different from a company's cryptographic primitive[255] becoming a standard that is accepted internationally. There are two issues involved. First, industry does not have organizational capacity in that only NIST can create a FIPS. Second, there is

---

[251] Camellia, a 128-bit block cipher, was a successful entrant in the NESSIE competition; see, e.g., Bart Preneel, NESSIE Project, in ENCYCLOPEDIA OF CRYPTOGRAPHY AND SECURITY (Henk C.A. van Tilburg, Sushil Jajodia, eds. 2011), 834. Note 160, *supra*, provides details on NESSIE, an E.U. effort to design new cryptographic primitives.

[252] Of the first seven cryptographers who won the Turing Award (computer science's equivalent of the Nobel), two—Shafi Goldwasser and Adi Shamir—were Israeli. The International Association for Cryptologic Research is the main professional organization for research cryptographers; of its first eighty-four fellows, fourteen are Israeli or Israeli born. INT'L ASS'N FOR CRYPTOLOGIC RSCH., https://www.iacr.org/fellows [https://perma.cc/XMY9-5TJ8] (last visited Jan. 21, 2022).

[253] The NSO Group is an Israeli company specializing in hacking tools for smartphones. *See* NSO GROUP, https://www.nsogroup.com [https://perma.cc/5HQE-LC8Y] (last visited Apr. 10, 2022). The company claims that its tools are sold to governments for use in counterterrorism and criminal investigations, but the company's tools have been repeatedly used against human rights workers, journalists, and dissidents. *See* Stephanie Kirchgaessner, Paul Lewis, David Pegg, Sam Cutler, Nina Lakhani & Michael Safi, *Revealed: leak uncovers global abuse of cyber-surveillance weapon*, GUARDIAN (July 18, 2021), https://www.theguardian.com/world/2021/jul/18/revealed-leak-uncovers-global-abuse-of-cyber-surveillance-weapon-nso-group-pegasus [https://perma.cc/Z9X4-MPWK]; *see also The Pegasus Project*, GUARDIAN, https://www.theguardian.com/news/series/pegasus-project [https://perma.cc/5FAF-J7RG]). In November 2021, the U.S. government placed the company on the "entity" list, which blocks it from purchasing components from U.S. firms without a special license. Addition of Certain Entities to the Entity List, 86 Fed. Reg. 60,759 (Nov. 4, 2021).

[254] Israeli cryptographers actively participate in both NIST and European cryptographic standardization efforts, but these efforts are not overseen by the Israeli government.

[255] Primitives include block ciphers, hash functions, additive stream ciphers, and digital signatures.

the issue of trust, that is, trust that the decision to standardize a particular algorithm will be made without bias.

There is a different problem for individual researchers, for instance cryptographers from academia. While individuals may not suffer as much from the trust issue that enterprises do, individual researchers lack organizational and technical capacity—and thus lack the capability—to run a proper vetting process needed for determining a cryptographic standard.

We now expand on these issues—but do not discuss Chinese or Russian efforts, since these are unlikely to be serious contenders for international standardization.

1. European Union Efforts in Civil-sector Cryptography

Europe has much technical expertise in cryptography, and the European Union (E.U.) has technical expertise and organizational trust. Rijndael, the algorithm that became AES, was developed by two Belgium cryptographers. As the home of an assortment of advanced democracies, Europe can lead an open and transparent process similar to the one by NIST. But this is unlikely to occur.

European policymakers tend to view cryptography as solely a national security issue, and not as a technology with economic implications.[256] This position makes little sense in 2022—or even a quarter century ago—given complex interdependencies between national economic and security issues. Despite the increasing role of the Internet in civilian life, European nations have largely refrained from developing cryptographic standards for non-national security purposes.[257] The viewpoint that cryptography is a national security technology somewhat ties the E.U.'s hands. That is because under Article 3(a)(2) of the 2007 Treaty of Lisbon, national security continues to remain outside the scope of the European Union. [258]

---

[256] Interview with Bart Preneel, Professor, Katholieke Universiteit Leuven (Apr. 18, 2019).

[257] Europe's lack of development of cryptographic standards for non-national security purposes is demonstrated by the lack of strong European infrastructure for developing such standards and by the opinion of both the European Commission and ENISA's Management Board. *See infra* note 264 for an explanation of Europe's lack of interest in developing non-national security cryptographic standards. There are, of course, exceptions. *See* note 160, *supra*, regarding the NESSIE project.

[258] Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community, art. 3(a)(2), Dec. 13, 2007, 2007 O.J. (C 306) ("The [European] Union . . . shall respect their essential State functions, including ensuring the territorial

Moreover, the lack of other major debacles involving cryptographic standards is partially why creating separate cryptographic standards for non-national security purposes has not been a priority for European nations. Thus, the development of a European standards organization would not be put on the E.U. agenda because of the principle of subsidiarity that precludes E.U. members from intervening into its member's national policies unless such intervention adds value. This principle also puts development of cryptographic standards outside E.U. competency.

U.S. allies have not viewed the U.S. government-developed cryptographic standards as a significant threat to their security or economies.[259] As for non-national security uses, a single-state solution is not very useful. The NIST standards work, and the E.U. nations rely on them. It would seem that in Europe, NIST is still seen as a rather neutral organization with a reputation for fairness.

There is a bit more to the story, however. There is a European effort on cryptographic standardization, but it is a relatively weak one: the European Union Agency for Cybersecurity (ENISA). Its role has been largely symbolic, with its original location in Crete—a location notably less convenient to reach and work in than others in the European Union—sending a clear signal of the unimportance of the agency's mission to Europe.[260] One researcher described ENISA's years in Crete as the organization "fighting for its existence."[261]

In 2013, however, the agency moved a third of its personnel to Athens. With this move, ENISA also obtained more resources, more recognition by E.U. member-states, and permanent status.[262] Yet despite this change, the agency has no present ability to obtain the resources or expertise that NIST has. Several senior European cryptographers noted that Germany, the U.K. (when it was a part of the E.U.), and France strongly opposed any cross-European effort on cryptographic standards, effectively keeping ENISA from acquiring the resources, expertise, and a proper process to vouch for an algorithm's security.[263] Given that Germany and France have stronger

---

integrity of the State, maintaining law and order and safeguarding national security. In particular, national security remains the sole responsibility of each Member State.").

[259] Interview with anonymous privacy and security researcher in Europe.

[260] *Id*.

[261] Interview with Steve Purser, head of the Core Operations Department at the European Union Agency for Cybersecurity (ENISA), September 4, 2019.

[262] Interview with Dan Bernstein & Tanja Lange (Mar. 12, 2019).

[263] The European Commission believes that it has no mandate to develop separate European standards aside from telecommunications standards developed by ETSI, which are of limited

domestic encryption expertise, they remain reluctant to put the security of their commercial communications in the hands of the less equipped ENISA, but rather prefer to maintain existing power dynamics.

Finally, the European academic community, which plays a more important role in cryptographic standards development than ENISA,[264] views NIST as an excellent arbiter for international cryptographic competitions. There is so far little movement to appreciably empower ENISA and many believe that it may take a long time before ENISA will have similar competency to NIST—if ever.[265]

Thus, although there is technical capacity and the potential for organizational capacity for developing a cryptographic standards organization in Europe, it is unlikely to occur. In the wake of the Dual_EC_DRBG situation, European leaders failed—and most likely had no interest—in developing an alternative cryptographic institution despite prime timing for such a change. Instead, they defaulted to giving their own standards organization, ENISA, a largely symbolic role. In doing so, they ensured continued reliance on U.S. cryptographic standards for non-national security matters, including business and industry communications.

2. Efforts by Non-state Actors in Civilian Cryptography

Lastly, we review efforts of some non-state groups who have tried developing standards, to become an international institution.

We start with the IETF and its parallel organization the IRTF. IETF develops many of the Internet communications protocols.[266] IETF started off in 1986 as a task force designed to identify and resolve engineering issues in the Advanced Research Projects Agency Network (ARPANET).[267] It has evolved a great deal since then, but its basic focus on engineering Internet protocols has not changed. This organization of engineers—and not mathematicians or cryptographers—lacks a formal membership roster or

---

scope. ENISA's Management Board shares this opinion, as do some members of its Advisory Board who are employed by U.S. companies. Interview with Bart Preneel, cryptographer and cryptanalyst professor, and Katholieke Universiteit Leuven, COSIC group (Apr. 1, 2019) and email communication with the author (Apr. 4, 2021).

[264] Interview with Steve Purser, *supra* note 261.

[265] Interview with privacy and security researcher.

[266] *Internet Standards*, INTERNET ENGINEERING TASK FORCE, https://www.ietf.org/standards/ [https://perma.cc/BED7-HXFG] (last visited Apr. 1, 2022).

[267] Scott Bradner, *IETF History*, YOUTUBE (Feb. 1, 2016), https://www.youtube.com/watch?v=_TlqisFpMGw [https://perma.cc/56V4-H2XH].

membership requirements[268] and the type of budget and government mandate that NIST has. Because it serves a different function, IETF is not a competitor of NIST.[269]

A parallel organization to IETF, IRTF, focuses on longer-term research issues. One of its groups, the Crypto Forum Research Group (CFRG), "provide[s] a forum for discussing and analyzing general cryptographic aspects of security protocols, and to offer guidance on the use of emerging mechanisms and new uses of existing mechanisms."[270] Although IRTF has a longer-term focus than the IETF, it is an organization whose functioning does not lend itself to the rigorous processes involved in developing cryptographic standards.[271]

Besides standards organizations, companies may also be able to have their internal standards adopted as industry standards (this constitutes a valuable win for the company). Occasionally even some researchers may take on the task. Their ability to do so is limited, but academics Dan Bernstein and Tanja Lange succeeded in the case of certain elliptic curves. We next examine how they were able to do so.

Dual_EC_DRBG was used for key exchange in TLS, the cryptographic protocol providing communications security for https, email, and other applications. Because NSA had a backdoor into the curve's parameters,[272] the curve needed to be replaced.[273] The question was which elliptic curve should be used in its stead.

---

[268] LAURA DENARDIS, THE GLOBAL WAR FOR INTERNET GOVERNANCE 69 (2014).

[269] Langley, *supra* note 205.

[270] *Crypto Forum Research Group*, INTERNET RSCH. TASK FORCE (Apr. 7, 2019), https://irtf.org/cfrg [https://perma.cc/A6NM-7UQH].

[271] AARON FALK, VERN PAXSON & SALLY FLOYD, INTERNET ARCHITECTURE BD., IAB THOUGHTS ON THE ROLE OF THE INTERNET RESEARCH TASK FORCE (IRTF), RFC 4440, at 5 (Mar. 2006), https://datatracker.ietf.org/doc/rfc4440 [https://perma.cc/8YYL-44AX].

[272] There was nothing wrong with the curve itself; the problem was that the NSA knew the relationship between two given parameters, and that allowed the agency to decrypt encrypted communications.

[273] *See* Julian E. Barnes & Helene Cooper, *Trump Discussed Pulling U.S. From NATO, Aides Say Amid New Concerns Over Russia*, N.Y. TIMES (Jan. 14, 2019), https://www.nytimes.com/2019/01/14/us/politics/nato-president-trump.html [https://perma.cc/6WCY-K74A]. The same curve could have been used for random bit generation, but with different points (parameters for encryption). But, with good reason, Dual_EC_DRBG was tainted in the public's eyes; the best thing to do was to replace the curve rather than just the two points.

Bernstein had one, Curve 25519, that he had publicly proposed in 2005 and for which he had made running code available. Bernstein and Lange analyzed different curves for security and computation speed, publishing code for the implementation.[274] While many forms of encryption need a long and careful vetting process, the curves that Bernstein and Lange proposed were part of a class the cryptographic community strongly believed to be secure.[275] That, and the fact that Bernstein had produced running code, made his proposed curve popular with implementers.[276]

There were competing proposals. In the mid-1990s, elliptic-curve cryptography was still relatively new; some standards bodies had concerns about its security. This was especially the case after researchers had shown that encryption based on certain types of elliptic curves did, in fact, have weaknesses.[277] To prevent such problems, the ANSI standards committee[278] decided to include curves generated "at random";[279] that would decrease the chance that selected curves belonged to a special, yet unknown,[280] class of easy-to-break curves.[281] Such a process serves two purposes: (i) anyone can check that the computation was properly done and (ii) yet, because the process is computationally infeasible to invert, it would be highly unlikely that the process could be manipulated to produce a curve that was found in one of the publicly unknown, problematic classes.[282]

NSA generated the curves for ANSI, and in 1997 NIST recommended fifteen of them for use by federal agencies.[283] The effort appeared fully

---

[274] EXPLICIT FORMULAS DATABASE, https://hyperelliptic.org/EFD/ [https://perma.cc/HY4E-U7B9] (last visited Apr. 1, 2022).

[275] *See* Menezes, *supra* note 10. This means avoiding "supersingular" curves and "prime-field anomalous elliptic."

[276] Paterson, *supra* note 233.

[277] *See* Menezes, *supra* note 10. Supersingular and prime-field anomalous elliptic curves have such problems.

[278] This was ANSI X9.F.1, which handles cryptographic standards for the financial sector.

[279] Randomization was achieved by using a "seed" and then running this seed through the hash function. Koblitz & Menezes, *supra* note 10, at 38.

[280] The issue was that the provider of the curve might know certain classes of curves had weaknesses, but that information would not be public. Then the curve provider could potentially provide such a curve to which they had a secret backdoor that no one else was aware existed.

[281] Koblitz & Menezes, *supra* note 10, at 38.

[282] *Id.*

[283] NAT'L INST. OF STANDARDS & TECH., DIGITAL SIGNATURE STANDARD (DSS), FIPS PUBLICATION186-2 24–48 (Jan. 27, 2000), https://csrc.nist.gov/csrc/media/publications/fips/186/2/archive/2000-01-27/documents/fips186-2.pdf [https://perma.cc/8ST2-UMKC]; *see also* Koblitz & Menezes, *supra* note 10, at 35.

aboveboard, and for sixteen years there were no complaints about those elliptic curves.[284] But in the wake of the Snowden disclosure about Dual_EC_DRBG,[285] some cryptographers also cast aspersions on the NIST curves.[286]

There was no evidence to support such claims. Although NSA had created the backdoored Dual_EC_DRBG, it is extremely unlikely that the agency engaged in the same type of chicanery with the 1997 NIST curves.[287] As cryptographers Neal Koblitz and Alfred Menezes observed, for one thing, the process by which the curves were arrived at was public—and thus easily checked.[288] Koblitz and Menezes pointed out that the curves were generated by NSA's Information Assurance Directorate, which, in the pre-9/11 period, had strongly pushed for secure solutions, not ones with cryptographic backdoors.[289] Moreover, as Koblitz and Menezes noted in 2016, no weaknesses had been found in the curves generated by NSA and recommended by NIST.[290] Nor have there been since.

Though the doubts about the NIST curves raised by this small group of cryptographers appeared to be without basis, the questions about the curves had an effect. Standards groups began to consider whether they should replace their recommended curves. And at Microsoft, researchers worked to develop a method for deterministically generating high-performance ECC curves, thus preventing a curve designer from having any ability to modify

---

[284] Koblitz & Menezes, *supra* note 10, at 36.

[285] Although the initial news articles did not explicitly mention Dual_EC_DRBG, because of details discussed in the article, cryptographers immediately knew which standard was the backdoored algorithm.

[286] *See* Bruce Schneier, *NSA Surveillance: A Guide to Staying Secure*, GUARDIAN (Sept. 6, 2013), https://www.theguardian.com/world/2013/sep/05/nsa-how-to-remain-secure-surveillance [https://perma.cc/6M3U-2V7S]; Dan Bernstein, *Rigidity*, SAFECURVES (Oct. 25, 2013), https://safecurves.cr.yp.to/rigid.html [https://perma.cc/FF82-FBLY].

[287] Koblitz & Menezes, *supra* note 10, at 36–38.

[288] *Id*.

[289] *See* Koblitz & Menezes, *supra* note 10, at 38. Brian Snow, the IAD technical director and one of the NSA employees who generated the curves, was the chair of the joint NIST-NSA Technical Working Group during the development of AES; his support was critical in the open process that occurred—*see supra* Part II.C for discussion of the NIST-NSA Technical Working Group); he and Mike Jacobs, the head of IAD, generated the curves. As Koblitz and Menezes note, IAD underwent a change post-9/11, during which Snow was eased out of the IAD position in 2002 and Jacobs retired.

[290] Koblitz & Menezes, *supra* note 10, at 38.

the curve.[291] Such curves would be trusted. Bernstein had laid his groundwork years before and had high-performance code running.[292]

Alphabet (Google) has also established a cryptography standard. In 2015, CFRG opened a call for the development of a cryptographic curve to be used in Internet protocols. Knowing that NIST had historically prioritized hardware standards development and that the process took a decade on average to develop similar standards for software, Google chose to establish a standard early. Using its own talent for determining the "right" elliptic curve for a key-exchange method for TLS, the team settled on the Bernstein Curve 25519.[293] The company did not first consult with CFRG, NIST, or anyone else—instead using its clout to determine which curve would become the de facto standard.

Google could not, *de jure*, establish an industry standard. The Microsoft research group had been putting together its own CFRG proposal, complete with a rigorous vetting process. But when the time came for the standards organizations to adopt new curves, despite the strong research reputation of the Microsoft scientists, some members of the cryptographic community were unwilling to accept the proposals developed by Microsoft Research's Security and Cryptography team, opting for the Bernstein curve instead.[294] Ultimately, however, Microsoft product teams chose to follow Google's lead, picking the de facto industry standard over their own company's efforts. Google effectively created an industry standard.

A notable lesson from the CFRG process is that in terms of cryptographic standardization, CRFG is not a competitor of NIST; these two organizations serve different functions. NIST competitions resemble a research process. NIST ensures that everyone's voice is heard, and the process includes a transparent and rigorous peer review. Members of the

---

[291] Joppe W. Bos, Craig Costello, Patrick Longa & Michael Naehrig, *Selecting Elliptic Curves for Cryptography: An Efficiency and Security Analysis*, 6 J. CRYPTOGRAPHIC ENG'G 1 *passim* (2016).

[292] Daniel J. Bernstein, *Curve 25519: New Diffie-Hellman Speed Records*, *in* PUBLIC KEY CRYPTOGRAPHY—PKC 2006 207 (Moti Yung, Yevgeniy Dodis, Aggelos Kiayias & Tal Malkin eds., 2006).

[293] Langley, *supra* note 4; *see also X25519 for TLS*, CHROME PLATFORM STATUS https://www.chromestatus.com/feature/5682529109540864 [https://perma.cc/AQ8P-NKA8] (last visited Apr. 1, 2022).

[294] Kenny Paterson, who co-chaired the CFRG at the time in question, said, "Some in the IETF and IRTF community privately reported their misgivings about proposals coming from Microsoft employees because of how they viewed that company's previous actions in IETF." Interview with Paterson, Professor of Information Security, Information Security Group at Royal Holloway, University of London (June 13, 2019).

cryptographic community, especially academics, are happy with this arrangement.[295] CFRG largely does not develop new standards or vet a new cryptographic algorithm's security. Rather, CFRG standardizes the use of an already agreed-upon and vetted algorithm. Paterson, who co-chaired CFRG, explained that the group focused on efficacy: Does the community believe this system will do well in a particular application? And will it be adopted?[296] That differing set of priorities is why the Microsoft proposal lost out to Google's fast-moving coup; a proof of security could not compete with an already widely deployed curve.

CFRG had been headed by several well-respected academics, but largely does not draw in the academic community—for the effort is not academic work. Given IRTF's lack of the rigorous processes involved in developing cryptographic standards. CFRG is not able to run large-scale competitions similar to those organized by NIST. Paterson said that CFRG could not, for example, run as complex an operation as NIST on finding "post-quantum" crypto standards to replace the algorithms currently in use.[297] In addition, industry's interest is on NIST because the FIPS are mandated for equipment sold for U.S. government use, which creates a large follow-on effect of widespread global adoption. But CFRG is nimbler and is focused on developers. As we have seen, that sometimes gives the organization an edge over NIST. And while CFRG's work was originally more akin to approving known standards for new uses rather than developing cryptographic standards *de novo*, increasingly the organization is developing standards from scratch.

Yet, despite this handful of examples, as we observed earlier, it is unlikely that industry can be the primary developer of cryptographic standards. There is a lack of organizational capacity. But the real problem with industry developing standards is trust in the fairness of decisions. And while individual researchers may not suffer as much from the trust issue, the Bernstein curve notwithstanding, they lack the organizational and technical capacity—and thus lack the capability—to run a proper vetting process needed for determining a cryptographic standard.

C. No One Can Step in for NIST

NIST brings organizational and technical support to the development of cryptographic standards. It has funding from the U.S. government, and while the NIST cryptographic effort was sorely underfunded in the early

---

[295] Langley, *supra* note 205.
[296] Paterson, *supra* note 233.
[297] *Id*.

years of FIPS development, that is not the case now.[298] Nor is it likely to be in the future; cybersecurity has simply become too important. NIST's study of the economic benefits that come to the United States from the development of cryptographic standards[299] is likely to ensure continued support from Congress for the Computer Security Division's effort.

Trust is another aspect as to why NIST is unlikely to be replaced by an agency in Europe or elsewhere. The NIST scientists not only went about rectifying the lacunae that enabled the NSA backdoor, but they also took responsibility for their failures, both in documents and public presentations.[300] NIST has handled cryptographic standards competitions in the way that NIST handles its efforts, with fairness, honesty, and transparency. And NIST CSD personnel have developed personal and professional relationships with cryptographers around the world.[301]

---

[298] Budgets for the Computer Security Division are not explicitly broken out by Congress, but some public data points demonstrate the increased federal commitment to the division's efforts. For example, NIST CSD's budget for fiscal year (FY) 2004 was about $9M USD. *See* NAT'L INSTITUTE OF STANDARDS & TECH., THE CASE FOR ADEQUATE FUNDING: A REPORT BY THE INFORMATION SECURITY AND PRIVACY ADVISORY BOARD 7 (June 2004), https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/correspondence/ISPAB-ReportAdequateFundingNIST-CSD.pdf [https://perma.cc/67LJ-NFPE]. But the Appropriations Committee estimate for 2015 included $15 million for NIST's Cybersecurity Center of Excellence, a government-industry partnership, $16.5 million for the National Strategy for Trusted Identities in Cyberspace effort, $4 million for NIST's National Initiative in Cybersecurity Education, and at least $60.7 million for cybersecurity research; this included an increase of $5 million over the previous year for work on cryptographic standards. S. REP. NO. 113-181, at 25–26 (2014). There are two divisions within NIST's Information Technology Laboratory with a cybersecurity mission, so about half of that sum is for the Computer Security Division (which handles cryptographic standards efforts). NIST CSD's budget for FY 2021 was $32 million USD. *See Hearing on SolarWinds and Beyond: Improving the Cybersecurity of Software Supply Chains*, 117th Cong. 9 (2021) (testimony of Matthew A. Scholl, Chief, Computer Security Division, Information Technology Laboratory, NIST).

[299] *See generally* Leech & Chinworth, *supra* note 210; Leech, Ferris & Scott, *supra* note 130.

[300] *See, e.g.*, KELSEY, *supra* note 46.

[301] Many of the world's cryptographers have continued to actively participate in NSA cryptographic activities since the Dual-EC-DRBG disclosures. *See, e.g.*, MOODY, *supra* note 188. But that in itself does not fully show the strength of the ties. It is perhaps better demonstrated by the support of senior leaders in cryptography and computer security for NIST. Vinton Cerf, who is recognized as one of "the fathers of the Internet," was very supportive of NIST, emphasizing the importance of adequate resources for the agency during his Committee of Visitor review post Dual-EC-DRBG. *See* NIST CRYPTOGRAPHIC STANDARDS AND GUIDELINES DEVELOPMENT PROCESS, *supra* note 155, at 1. Lipner noted that "Both [the AES and SHA-3] competitions attracted worldwide participation and attention from the academic community and industry and were widely seen as fair and well-executed. These competitions organized and managed by NIST are examples of best practices in the development of cryptographic standards." Steven B. Lipner, *Report of Steven*

A replacement for NIST would have to duplicate its capabilities and earn the trust that NIST has accumulated. This would not be an easy task.

IV. BUT WILL THIS SITUATION LAST?

The fact that NIST is running competitions for Lightweight Cryptography[302] and Post-Quantum cryptographic standards,[303] and that these standardization efforts have international support, lends credence to the idea that NIST will continue to lead in developing cryptographic standards adopted internationally. A NIST skeptic could note that, in the aftermath of the Snowden disclosures, the E.U. explored "technological sovereignty,"[304] using concerns about U.S. surveillance and the privacy rights of European citizens as a catalyst for employing a combination of regulation and incentives as a way to develop European technology in privacy and security. But as we have seen, there was little European appetite for setting up a serious competitor to NIST's role.[305] By 2015, NIST and the cryptographers had settled back into a comfortable and mutually beneficial set of roles. Were the world still in *Pax Americana*, much like the period that prevailed from the late 20th century,[306] NIST's role would likely have been successfully reestablished and stayed that way. But the world is considerably less stable than during that period.

B. Lipner to the NIST VCAT Subcommittee on Cybersecurity, *in* NIST CRYPTOGRAPHIC STANDARDS AND GUIDELINES DEVELOPMENT PROCESS, *supra* note 155, at 4; *see also* Bart Preneel, *Comments on the NIST Cryptographic Standards and Guidelines Development Program*, *in* NIST CRYPTOGRAPHIC STANDARDS AND GUIDELINES DEVELOPMENT PROCESS, *supra* note 155, at 7 ("The confidence of the [academic and industrial] community has NIST had increased in the past 15 years after the excellent work performed by NIST during the AES and SHA-3 competitions.").

[302] Meltem Sonmez Turan, *Lightweight Crypto, Heavyweight Protection*, NAT'L INST. OF STANDARDS & TECH. (Jan. 13, 2021), https://www.nist.gov/blogs/taking-measure/lightweight-crypto-heavyweight-protection [https://perma.cc/E3KN-SUHC].

[303] *NIST Reveals 26 Algorithms Advancing to the Post-Quantum Crypto Semifinals*, NAT'L INST. OF STANDARDS & TECH. (Jan. 30, 2019), https://www.nist.gov/news-events/news/2019/01/nist-reveals-26-algorithms-advancing-post-quantum-crypto-semifinals [https://perma.cc/5GRF-LDUR].

[304] EUR. COMM'N, SHAPING EUROPE'S DIGITAL FUTURE 1 (2020), https://ec.europa.eu/info/sites/info/files/communication-shaping-europes-digital-future-feb2020_en_4.pdf [https://perma.cc/8V77-WT2S].

[305] There was no possibility for an Asian competitor to NIST; Asia lacks a venue similar to EU's ENISA that can host such an initiative.

[306] *See* Charles A. Kupchan. *After Pax Americana: Benign Power, Regional Integration, and the Sources of a Stable Multipolarity*, 23 INT'L SEC. 40 *passim* (1998) (broadly discussing unipolarity).

The election of Donald Trump and his subsequent actions as President, including withdrawals from the Paris Agreement,[307] the Joint Comprehensive Plan of Action on Iran's nuclear program,[308] the United Nations Human Rights Council,[309] and the World Health Organization,[310] the refusal to sign the Trans-Pacific Partnership,[311] threats of withdrawal from the North Atlantic Treaty Organization,[312] trade tariffs imposed on European steel and aluminum,[313] and the lack of pushback from the Republican party, created serious concerns of a massive shakeup in the world order that had existed since 1945. European diplomats privately identified the Trump presidency as the lowest point in transatlantic relations since the end of the Cold War. There is now a wariness about trusting U.S. promises that did not exist over the previous seventy-five years.[314] Trump's presidency served as a wake-up call for the E.U. leaders about the importance of re-establishing the union's position as an economic power.[315]

---

[307] Timothy Cama & Devin Henry, *Trump: We are getting out of Paris climate deal*, HILL (June 1, 2017), https://thehill.com/policy/energy-environment/335955-trump-pulls-us-out-of-paris-climate-deal [https://perma.cc/9AFD-NGHY].

[308] *Read the Full Transcript of Trump's Speech on the Iran Nuclear Deal,* N.Y. TIMES (May 8, 2018), https://www.nytimes.com/2018/05/08/us/politics/trump-speech-iran-deal.html [https://perma.cc/S2J2-RWG6].

[309] *US quits 'biased' UN human rights council,* BBC NEWS (June 20, 2018), https://www.bbc.com/news/44537372 [https://perma.cc/8RQP-Q6DR].

[310] Rafi Letzter, *The US formally announced its withdrawal from the World Health Organization*, LIVE SCIENCE, (July 7, 2020), https://www.livescience.com/trump-exits-who-united-states.html [https://perma.cc/RP2X-4VTX].

[311] *See* Joseph Chinyong Liow, *US–Southeast Asia Relations under the Trump Administration*, 24 ASIA POLICY 53, 53–58 (2017).

[312] Barnes & Cooper, *supra* note 273.

[313] David J. Lynch, Josh Dawsey & Damian Paletta, *Trump imposes steel and aluminum tariffs on the E.U., Canada and Mexico,* WASH. POST (May 31, 2018), https://www.washingtonpost.com/business/economy/trump-imposes-steel-and-aluminum-tariffs-on-the-european-union-canada-and-mexico/2018/05/31/891bb452-64d3-11e8-a69c-b944de66d9e7_story.html [https://perma.cc/JUV7-XW2V].

[314] Kristian L. Nielsen & Anna Dimitrova, *Trump, trust and the transatlantic relationship*, 42 POLICY STUDIES 699, 708 (2021); Florian Böller, *A Breakdown of Trust: Trump, Europe and the Transatlantic Security Community*, *in* MOBILIZATION, REPRESENTATION, AND RESPONSIVENESS IN THE AMERICAN DEMOCRACY 301–319 (2019).

[315] Trump's actions also made Europeans start thinking strategically of their "military sovereignty," to use a term of French President Emmanuel Macron. *Emmanuel Macron warns Europe: NATO is becoming brain-dead,* ECONOMIST (Nov. 7, 2019), https://www.economist.com/europe/2019/11/07/emmanuel-macron-warns-europe-nato-is-becoming-brain-dead [https://perma.cc/BEP7-BPZ4].

Yet for the reasons we have previously articulated,[316] it is unlikely that Europe—and, in particular, the E.U.—will split from the U.S. in non-national security encryption standards.[317] Use of NIST cryptographic standards in the civil sector is beneficial to their economies and, as described earlier, developing an E.U. standards organization is complex for many reasons.

The image and prestige of the United States, which had been falling gradually for some time, also took a sharp dip among many Asian countries during the Trump era.[318] Despite a significant warm-up in the relationship between the U.S. and certain Asian countries during the Biden administration, many Asian politicians continue expressing caution and distrust in the U.S. political system, given the significant changes in the U.S. domestic political situation.[319] This would not concern NIST's role in providing internationally accepted encryption standards but for nascent actions by China in the Internet standards world.[320]

The Internet was designed with the assumption that the underlying communications function can only be completely and correctly implemented by the application and not by the communications infrastructure (though the communications system may provide some performance enhancement); this is known as the end-to-end principle.[321] This model, which has permitted vast numbers of innovative end-user technologies to be quickly and easily developed, enables the use of end-to-end encryption in TLS, email, and other applications.

Instead of this application-centric model of Internet architecture, China is championing a "network-centric" Internet that would enable fine-

---

316 *See supra* Part III.B.1.

317 Splitting on encryption policy is more likely; the United States, at present, does not appear to be moving towards controls on use of encryption in consumer products, while some European politicians are pressing for exactly that.

318 Richard Wike, *The Trump era has seen a decline in America's global reputation,* PEW RSCH. CTR. (Nov. 19, 2020), https://www.pewresearch.org/fact-tank/2020/11/19/the-trump-era-has-seen-a-decline-in-americas-global-reputation/ [https://perma.cc/25XW-BM45].

319 Alex Fang, Marrian Zhou & Francesca Regalado, *Team Biden says America is back. But is Asia ready to welcome it,* NIKKEI ASIA (Dec. 2, 2020), https://asia.nikkei.com/Spotlight/The-Big-Story/Team-Biden-says-America-is-back.-But-is-Asia-ready-to-welcome-it [https://perma.cc/75AU-2EF8].

320 *See generally* Stacie Hoffmann, Dominique Lazanski & Emily Taylor, *Standardising the splinternet: how China's technical standards could fragment the Internet,* 5 J. CYBER POL'Y 239 (2020).

321 J.H. Salzer, D.P. Reed & D.D. Clark, *End-to-End Arguments in System Design*, 2 ACM TRANSACTIONS IN COMPUTER SYSTEMS 277 (1984).

grained controls on how people and things connect and communicate.[322] China has run the "Chinese" Internet since it first connected, separating itself through applications of censorship and control of companies and Internet service providers that can operate in China.[323] China is now seeking to exert control outside its border as well.[324] China's proposals for the network-centric Internet include what Huawei describes as a "tradeoff between accountability and privacy"[325] but that is in fact a network in which anonymity is no longer possible; this so-called "accountable network" is a surveillance network in disguise. China's new effort involves presentations in the International Telecommunications Union and the IETF; it represents a strong intent to reshape the Internet as opposed to simply controlling the network within China.[326]

The nation is also simultaneously pursuing the development of cryptographic standards. Appearing to compete with NIST, China has, for example, set up its own post-quantum cryptographic competition. It does not have to succeed directly through international adoption of its cryptographic standards. China can instead proceed in "stealth" mode though the use of its Belt and Road Initiative (BRI) by introducing its technology into other nations.[327]

Russia is also seeking to disrupt the end-to-end architecture in favor of a more controlled network-centric model, though the nation does not have the foreign reach that China has developed through BRI. At the same time, it appears that Russia is making efforts to have its cryptographic standards adopted more broadly. Some of these proposed standards are untrusted by the cryptographic research community.[328]

---

[322] *See* Hoffmann, Lazanski & Taylor, *supra* note 320.

[323] Henry L. Hu, *The Political Economy of Governing ISPs in China: Perspectives of Net Neutrality and Vertical Integration*, 207 CHINA Q. 523, 523–40 (2011).

[324] *See* Hoffmann, Lazanski & Taylor, *supra* note 320, at 240.

[325] Sheng Jiang, New IP Networking for Network 2030, Presentation at the Fifth ITU Workshop on Network 2030 16 (Oct. 15. 2019), https://www.itu.int/en/ITU-T/Workshops-and-Seminars/2019101416/Documents/Sheng_Jiang_Presentation.pdf [https://perma.cc/CM8K-NCY6].

[326] *See* Hoffmann, Lazanski & Taylor, *supra* note 320, at 242–245.

[327] *See id.* at 254.

[328] Joseph Cox, *Experts Doubt Russian Claims that Cryptographic Flaw was a Coincidence*, VICE (May 8, 2019), https://www.vice.com/en/article/43j3wm/experts-doubt-russian-encryption-standard-cryptography-backdoor-streebog-kuznyechik [https://perma.cc/H9XS-Y9TV]; Léo Perrin, *Partitions in the S-box of Streebog and Kuznyechik*, 2019 IACR TRANSACTIONS ON SYMMETRIC CRYPTOGRAPHY 302, 302 (2019); Léo Perrin, *Update on the ISO Standardization of Kuznyechik*, Report from Dagstuhl Seminar 20041 (Jan. 2020), https://who.paris.inria.fr/Leo.Perrin/slides/slides-dagstuhl-2020.pdf [https://perma.cc/38B9-

Thus, there are concerted efforts by U.S. adversaries to take the open Internet and transform it into an international communications network with exceedingly powerful surveillance capabilities. This potential transformation, even if it only partially succeeds, has many implications about the security of communications and the continued existence of a single connected global Internet and many "splinternets."

The potential for the transformation of the Internet increases the importance of NIST cryptographic standards to U.S. national security. These standards have been a form of soft power and have provided benefits to the U.S. economy.[329] Because their worldwide acceptance has enabled international communications to travel securely over a highly insecure network, the standards have played an important role in U.S. national and economic security. Cryptographic standards developed by NSA would not have played such a role; they would not have been trusted. NIST standards were—and continue to be.

Standards are an international affair, and NIST has always worked in an international realm. The agency is now expanding its international footprint in cybersecurity by making its cybersecurity offerings more easily accessible to other nations.[330] The Department of Commerce agency understands its role in promoting U.S. interests even if NSA has not always appreciated the function that NIST plays.

For decades, NSA fought NIST's role in developing cryptographic standards. When Congress passed the *Computer Security Act* in 1987, NSA

WZU8]; REPORT FROM DAGSTUHL SEMINAR 16021: SYMMETRIC CRYPTOGRAPHY (Joan Daemen, Tetsu Iwata, Nils Gregor Leander & Kasia Nyberg eds., 2018). The algorithms in question were designed by the Center for Information Protection and Special Communications of the Federal Security Service, which is Russia's main security agency. Kuznyechik was withdrawn for consideration for ISO standardization.

Russia is not the only nation in which such a situation has occurred. NSA sought ISO standardization for two symmetric-key ciphers, Simon and Speck. The agency's continued refusal to explain the security rationale behind the algorithms' design eventually led to a rejection. Tomer Ashur & Atul Luykx, *An Account of the ISO/IEC Standardization of the Simon and Speck Block Cipher Families*, *in* SECURITY OF UBIQUITOUS COMPUTER SYSTEMS: SELECTED TOPICS 63 (Gildas Avoine & Julio Hernandez-Castro eds., 2021).

[329] *See generally* Leech & Chinworth, *supra* note 210; Leech, Ferris & Scott, *supra* note 130.

[330] *International Cybersecurity and Privacy Resources*, NAT'L INST. OF STANDARDS & TECH. (Dec. 16, 2021), https://www.nist.gov/cybersecurity/international-cybersecurity-and-privacy-resources [https://perma.cc/N969-RBRK].

felt it had been blindsided.[331] Little over a decade later, as strong encryption became widely available to governments around the world, NSA shifted greater attention to computer network exploitation. NSA appeared to come to terms with NIST's role as the purveyor of civil-sector cryptographic standards, including for use in confidentiality. But the two agencies, appearing to complement each other's mission, were, as the Dual_EC_DRBG incident showed, actually competing—although NIST was sometimes blindfolded during the contest. NIST—through a careful, thorough, and energetic effort—appears to have recovered from the Dual_EC_DRBG incident. The agency learned to "[t]rust, but verify" by creating transparency needed for the research community to verify the strength of encryption standards. NIST developed new capabilities and expertise, and its efforts appear to be flourishing.

The national security threats that the United States faces are more complex than those that occurred when NSA was launching the Dual_EC_DRBG effort.[332] The U.S. faces a world in which the soft power provided by NIST—not just the deployment of its cryptographic standards, but also its model of open cryptographic standards competitions and honest brokering—contributes to U.S. national security. It is in the U.S.'s national-security interest—and thus ought to be in NSA policy—to fully and decisively support NIST's efforts in developing strong cryptographic standards. This is an interesting turn of affairs for both NSA and NIST, for the latter now provides national security, in a soft-power way, for the U.S.

---

[331] Clinton Brooks, Special Assistant to the Director of the NSA, wrote a memo that said, "In 1982, NSA engineered a National Security Decision Directive, NSDD-145, through the Reagan Administration that gave responsibility for the security of all information systems to the Director of NSA, eliminating NBS [National Bureau of Standards] from this . . . .This also stated we would assist the private sector. This was viewed as Big Brother stepping in and generated an adverse reaction . . . . Representative Jack Brooks, chairman of the House Government Operations Committee, personally set out to pass a law to reassert NBS's responsibility for Federal unclassified systems and to assist the private sector. . . . By the time we fully recognized the implications of Brooks' bill, he had it orchestrated for a unanimous consent voice vote package." EPIC CRYPTOGRAPHY AND PRIVACY SOURCEBOOK: DOCUMENTS ON WIRETAPPING, CRYPTOGRAPHY, THE CLIPPER CHIP, KEY ESCROW AND EXPORT CONTROLS 8–13 (David Banisar ed., 1996).

[332] OFF. OF THE DIR. OF NAT'L INTELLIGENCE, ANNUAL THREAT ASSESSMENT OF THE U.S. INTELLIGENCE COMMUNITY (2021), https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf [https://perma.cc/F333-ZTJP].