BREAKING ENCRYPTION AND GATHERING DATA: INTERNATIONAL LAW APPLICATIONS

Grant Hodgson[*]

[*] J.D. Candidate, J. Reuben Clark Law School, 2016. The Author would like to thank Eric Talbot Jensen for his guidance.

I. INTRODUCTION

In the early 1970s, the United States began using submarines to place recording devices on an underwater sea cable off the coast of Eastern Russia.[1] The cable transported communication between two Russian bases and every so often the United States would retrieve the recordings and listen for useful information.[2] The operation was known as Ivy Bells and although it was discontinued in 1981,[3] the technique of tapping underwater sea cables to gather information is still used today.[4] Governments use many methods to gather data as they try to guard against terrorist attacks and otherwise protect national security.[5] Non-state actors and states often try to prevent their communications and other data from being read by encrypting it.[6] For example, HTTPS[7] and SSL[8] are commonly used together to encrypt data traveling over the internet.[9]

[1] Olga Khazan, *The Creepy, Long-Standing Practice of Undersea Cable Tapping*, ATLANTIC (July 16, 2013), http://www.theatlantic.com/international/archive/2013/07/the-creepy-long-standing-practice-of-undersea-cable-tapping/277855/.

[2] *Id.*

[3] *See id.* (An NSA employee sold information about the program to the KGB).

[4] *New Nuclear Sub Is Said to Have Special Eavesdropping Ability*, N.Y. TIMES (Feb. 20, 2005), http://www.nytimes.com/2005/02/20/politics/new-nuclear-sub-is-said-to-have-special-eavesdropping-ability.html.

[5] Charlie Savage, Edward Wyatt & Peter Baker, *U.S. Confirms that It Gathers Online Data Overseas*, N.Y. TIMES (June 6, 2013), http://www.nytimes.com/2013/06/07/us/nsa-verizon-calls.html?pagewanted=all.

[6] *See* Press Release, Blue Coat Systems, Inc., *Blue Coat Launches Encrypted Traffic Management Ready Certification Program* (Mar. 3, 2015), *available at* https://www.bluecoat.com/company/press-releases/blue-coat-launches-encrypted-traffic-management-ready-certification-program (discussing the use of encryption by certain non-state actors).

[7] Jennifer Kyrnin, *What is HTTPS – Why Secure a Web Site*, ABOUT, http://webdesign.about.com/od/ecommerce/a/aa070407.htm (last visited Nov. 28, 2014).

[8] *What Is SSL (Secure Sockets Layer) and What Are SSL Certificates?*, DIGICERT, https://www.digicert.com/ssl.htm (last visited Nov. 28, 2014).

[9] Press Release, Blue Coat Systems, Inc., *Blue Coat Launches Encrypted Traffic Management Ready Certification Program* (Mar. 3, 2015), *available at* https://www.bluecoat.com/company/press-releases/blue-coat-launches-encrypted-traffic-management-ready-certification-program.

States are interested in developing encryption techniques that no one else can break while maintaining techniques that can break encrypted data created by other states.[10] For example, the European Union, Switzerland, and the NSA are all trying to develop quantum computing, which may be useful for breaking encryption.[11]

The international law principle of sovereignty applies to territorial decryption activities and provides guidance on when a state may break the encryption on messages sent by other states.[12] However, breaking encryption on data that is traveling on the high seas or traveling within a state's territory does not violate sovereignty.[13] This is true for every method of breaking encryption that I discuss in this paper. However, states must be careful of communications that meet the diplomacy and consular protection requirements and must leave these communications alone if they are found.[14] States may also share data gathered from their territory with other states without violating sovereignty.[15] Finally, there is no consensus on whether defeating encryption by installing malware on computers in foreign states violates sovereignty or not.[16] Current state practice seems to suggest, however, that it is not a violation of sovereignty.[17]

In Part II, I will explain the basics of encryption, networking, and how data travels over the internet securely. In Part III, I will explain the aspects of sovereignty that are most applicable to breaking encryption and tapping fiber optics cables on the high seas. In Part IV, I will discuss several techniques for gathering data and breaking encryption[18] that may

[10] *NSA Encryption*, PRODUCTS CRYPTO MUSEUM, http://www.cryptomuseum.com/crypto/usa/nsa.htm (last visited Nov. 28, 2014).

[11] Steven Rich & Barton Gellman, *NSA Seeks to Build Quantum Computer that Could Crack Most Types of Encryption*, WASH. POST (Jan. 2, 2014), http://www.washingtonpost.com/world/national-security/nsa-seeks-to-build-quantum-computer-that-could-crack-most-types-of-encryption/2014/01/02/8fff297e-7195-11e3-8def-a33011492df2_story.html.

[12] Wolf Heintschel von Heinegg, *Territorial Sovereignty and Neutrality in Cyberspace*, 89 INT'L L. STUD. 123, 126–27 (2013).

[13] *See* INT'L GROUP OF EXPERTS, TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE 16–18 (Michael N. Schmitt ed., 2013) [hereinafter TALLINN MANUAL] (discussing principles of sovereignty as they relate to cyber law); U.N. Convention on the Law of the Sea arts. 86, 89, Dec. 10, 1982, 1833 U.N.T.S. 397, *available at* http://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf.

[14] TALLINN MANUAL, *supra* note 13, at 26; Vienna Convention on Consular Relations art. 27, Apr. 24, 1963, 596 U.N.T.S. 261 [hereinafter Vienna Convention].

[15] Inaamul Haque & Ruxandra Burdescu, *Monterrey Consensus on Financing for Development: Response Sought from International Economic Law*, 27 B.C. INT'L COMP. L. REV. 219, 249 (2004).

[16] TALLINN MANUAL, *supra* note 13, at 16.

[17] *See* Hiroshi Shinotsuka, *How Attackers Steal Private Keys from Digital Certificates*, SYMANTEC (Feb. 22, 2013), http://www.symantec.com/connect/blogs/how-attackers-steal-private-keys-digital-certificates (discussing how multiple states use malware).

[18] The techniques include brute force attacks, man in the middle attacks that require the

be in use by states today, and how the law applies to each technique. I will discuss which scenarios do not violate sovereignty and which scenarios do violate sovereignty.

II. ENCRYPTION AND ROUTE SELECTION FOR DATA TRAVELING ON THE INTERNET

A. *How Data Is Encrypted*

Cryptology is the science of making and breaking codes.[19] It includes cryptography, or making codes, and cryptanalysis, the breaking of codes.[20] The original, readable message is known as the plaintext.[21] Unreadable text that comes from encrypting the plaintext is known as ciphertext.[22] Decryption is the act of converting the ciphertext into plaintext using a key.[23] When encrypting and decrypting a message, a key is necessary to make a cryptographic algorithm work correctly.[24] The key is typically a special number that is used by an algorithm.[25] Anyone that possesses a key that was used to encrypt some data is able to decrypt the same data using the key.[26] The key must be kept secret, otherwise anyone would be able to decrypt the ciphertext.[27] In a good cryptographic system, the algorithm used does not need to be secret because the security of the encryption depends only on the secrecy of the key.[28] To explain cryptography, assume Alice and Bob want to communicate with each other, and Eve is eavesdropping on their communication channel, whatever the channel may be.[29] It is assumed that Eve is able to intercept

cooperation of certificate authorities, stealing cryptographic keys, taking advantage of predictable random number generators, side-channel attacks, and submarine tapping. *See Making and Breaking Codes*, ARIZ. ST. U., http://cactus.eas.asu.edu/partha/Columns/03-19-encryption.htm (last visited Mar. 21, 2015) (discussing different techniques to break code).

[19] MARK STAMP & RICHARD M. LOW, APPLIED CRYPTANALYSIS-BREAKING CIPHERS IN THE REAL WORLD 2 (2007).

[20] *Id.*

[21] *Id.*

[22] JAMES F. KUROSE & KEITH W. ROSS, COMPUTER NETWORKING A TOP DOWN APPROACH 691 (5th ed. 2010).

[23] STAMP & LOW, *supra* note 19, at 2.

[24] KUROSE & ROSS, *supra* note 22, at 692.

[25] Margaret Rouse, *Key*, TECHTARGET, http://searchsecurity.techtarget.com/definition/key (last visited Mar. 23, 2015).

[26] *Id.*

[27] STAMP & LOW, *supra* note 19, at 2.

[28] NIELS FERGUSON ET AL., CRYPTOGRAPHY ENGINEERING 24 (2010) (Describing how keeping the algorithm secret is more difficult and expensive because it is built into the hardware or software making it harder to change if necessary).

[29] *Id*.

every message that Alice and Bob send to each other. To protect their communication, Alice and Bob agree on a secret key via some channel that Eve cannot eavesdrop on. The key is used to create ciphertext (encrypt the messages) that Alice and Bob send back and forth to each other.[30] When Bob receives the encrypted message he uses a decryption function to convert it into plaintext.[31] When Eve intercepts the message she will not be able to figure out anything more than the approximate length of the message and the time it was sent.[32] These principles have applications beyond just the transfer of communication. For example, stored data is also often encrypted in case it is ever stolen.[33]

Public key encryption is a widely used form of encryption. In public key encryption, Bob generates a pair of keys using a special algorithm.[34] One of the keys is used to encrypt data and the other key is used to decrypt data.[35] Bob publishes the encryption key so everyone can use it to encrypt messages or data.[36] Bob, however, keeps the decryption key secret.[37] When Alice wants to send a message to Bob she encrypts the message with the public key to get the cipher text.[38] Bob can then use his secret key and the decryption algorithm to decrypt the message.[39] In the real world, people and businesses need to communicate with many other parties securely. As scale increases, it becomes more difficult to keep track of all the keys that different parties are using.[40] Certificate authorities are used to make sure that a key is really Bob's key and not something Eve published while impersonating Bob.[41] A certificate authority is typically a trusted, third-party company.[42] It signs the public key using a digital signature allowing Alice to verify that the public key actually belongs to Bob.[43] Certificate authorities allow cryptography to work on a large scale.[44]

[30] *Id.*

[31] *Id.* at 28.

[32] *Id.* at 24.

[33] *Id*.

[34] *Id.* at 28.

[35] *Id.*

[36] *See* MARK STAMP, INFORMATION SECURITY PRINCIPLES AND PRACTICE 20 (2011).

[37] *Id.*

[38] FERGUSON ET AL., *supra* note 28, at 28.

[39] *Id.*

[40] *Id*. at 181.

[41] *Id*. at 30.

[42] There are many companies that act as certificate authorities including VeriSign, Comodo, and GoDaddy.

[43] FERGUSON ET AL., *supra* note 28, at 30.

[44] *A Cryptography Policy Framework for Electronic Commerce: Building Canada's Information Economy and Society*, Industry Canada (1998).

B. *Use of Cryptography on the Internet—Secure Sockets Layer (SSL)*

Secure Sockets Layer (SSL) and Transport Layer Security (TLS),[45] provide "confidentiality, data integrity, and end-point authentication [to the server and client]."[46] SSL is used by nearly all websites that allow commercial transactions (this includes Amazon, eBay, Yahoo!, MSN, and essentially all banks).[47] When a website is using SSL, a padlock icon appears in the browser near the URL and the URL starts with "https" instead of http.[48]

The following example is borrowed from Kurose & Ross and helps explain the need for SSL.[49] A normal guy named Bob wishes to buy shoes from Alice incorporated, a company that has a website to facilitate purchases. The Alice Incorporated site allows Bob to select the shoe style and quantity desired and to input his address and credit card number. Bob submits his information and expects to receive the shoes he ordered and a charge for his order on his credit card.[50] This type of online purchase would not work if Bob and Alice Incorporated did not use security measures.[51] If encryption is not used, an attacker Eve, could intercept Bob's order and obtain his payment card information.[52] Eve would then be able to use Bob's credit card to make her own purchases.[53] If some form of data integrity is not used, Eve could change any aspect of Bob's order. She could make him purchase two pairs of shoes instead of only one or change the mailing address.[54] If some form of server authentication is not used, Eve could pretend to be Alice Incorporated and make a server display Alice Incorporated's famous logo.[55] After Bob submits his order, Eve could take Bob's money and run.[56] In addition, Eve could commit identity theft by using the information that Bob submitted.[57]

SSL is a transport protocol that allows data to be exchanged over the internet securely and has three phases called the handshake, key

[45] TLS is a slightly modified version of SSL version 3. I will refer to both SSL and TLS as SSL.

[46] KUROSE & ROSS, *supra* note 22, at 94.

[47] *Id*. at 727.

[48] *Id.*

[49] For the original example, see *id.* at 727–28.

[50] *Id*.

[51] *Id.*

[52] *Id.* at 728.

[53] *Id.*

[54] *Id.*

[55] *Id.*

[56] *See id.*

[57] *See* Amadou Diallo, *How to Avoid Data Theft When Using Public Wi-FI,* FORBES (Mar. 23, 2015), http://www.forbes.com/sites/amadoudiallo/2014/03/04/hackers-love-public-wi-fi-but-you-can-make-it-safe/ (describing how SSL can create privacy and security for internet users).

derivation, and data transfer phases.[58] Throughout the following discussion, Bob is the client and Alice is the server. Alice has a private/public key pair and a certificate that "binds her identity to her public key."[59]

For this Article, the handshake phase is the most important part of SSL to understand. During the handshake phase Bob needs to (1) connect with Alice; (2) confirm that Alice is really Alice; (3) and send Alice a master secret key, which will be used to create other keys needed for the SSL session.[60] To start the handshake, Bob sends a hello message.[61] Alice sends back her certificate containing her public key.[62] Understanding the certificate is essential to understanding man in the middle attacks (one method to circumvent encryption) which will be discussed in Part IV. If Bob is able to confirm the certificate that Alice sent him with a Certificate Authority then he will trust Alice and the transaction will continue (this is essentially all done automatically by the software).[63] If the certificate is not confirmed by the Certificate Authority then an error message will be given.[64]

Next, Bob generates the master secret key (MS) that will be used for the current SSL session.[65] Bob encrypts the MS with Alice's public key and sends it to Alice.[66] Alice is able to decrypt the MS with her private key.[67] Thus, only Bob and Alice know the MS for this SSL session.[68] During the handshake phase Bob and Alice agree on which cryptographic algorithms to use.[69] RSA and Diffie-Hellman are commonly used algorithms in public key cryptography.[70] Alice and Bob next use the MS to generate several keys to use throughout the SSL session.[71] Now Bob and Alice can send data back and forth over the internet safely.[72]

[58] KUROSE & ROSS, *supra* note 22, at 729.

[59] *Id*. at 730–31.

[60] STAMP, *supra* note 36, at 354.

[61] *Id.*

[62] KUROSE & ROSS, *supra* note 22, at 730–31.

[63] *Id.* at 729–30.

[64] *Securing Communications with Secure Socket Layer (SSL)*, MICROSOFT, http://msdn.microsoft.com/en-us/library/dd163531.aspx (last visited Nov. 23, 2015).

[65] KUROSE & ROSS, *supra* note 22, at 730.

[66] *Id.*

[67] *Id.*

[68] *Id.*

[69] *Id.* at 732.

[70] Margaret Rouse, *RSA Algorithm (Rivest-Shamir-Adleman)*, TECHTARGET, http://searchsecurity.techtarget.com/definition/RSA (last visited Nov. 28, 2014) (describing how RSA works); Margaret Rouse, *Diffie-Hellman Key Exchange (exponential key exchange)*, TECHTARGET, http://searchsecurity.techtarget.com/definition/Diffie-Hellman-key-exchange (last visited Nov. 28, 2014) (describing Diffie-Hellman).

[71] KUROSE & ROSS, *supra* note 22, at 730.

[72] *Id.* at 731.

C. *Networking and How Data Travels Over the Internet*

The boundaries of a state's territory play an important role in international law and serve a key role in delineating a state's exercise of sovereignty. To determine whether international law is violated when data is intercepted while traveling through the internet, it is important to understand how data travels. The simple truth is that the protocols used by the internet in no way take into account the physical location of states' borders. The internet today is based on the Open Systems Interconnection (OSI) model.[73] It contains seven layers.[74] The third layer of OSI is known as the network layer and it determines the path that packets[75] take from senders to receivers.[76] There are two main routing algorithms that determine the paths of packets.[77] The first algorithm determines how data travels within a network or within an autonomous system (AS).[78] "An AS is a collection of routers whose prefixes and routing policies are under common administrative control."[79] For example, a university or business will often operate its own AS.[80] The second routing algorithm determines how data travels between one AS and another.[81]

If a router is not directly connected to the destination address, it must send the data along a path hopping from router to router until it reaches the destination address.[82] Thus, as data travels over the internet it hops from router to router until it reaches its final destination.[83] Routers within an AS all use the same routing algorithm and they know information about each other.[84] They communicate with each other periodically to update who their neighbors are and to find out possible routes.[85]

[73] *The Open System Interconnection (OSI) Reference Model*, THE TCP/IP GUIDE, http://www.tcpipguide.com/free/t_TheOpenSystemInterconnectionOSIReferenceModel.htm (last visited Nov. 28, 2014).

[74] *Id.*

[75] Data travels over the internet in packets. *See* Margaret Rouse, *Packet*, TECHTARGET, http://searchnetworking.techtarget.com/definition/packet (last visited Nov. 28, 2014).

[76] *The Open System Interconnection (OSI) Reference Model*, THE TCP/IP GUIDE, http://www.tcpipguide.com/free/t_TheOpenSystemInterconnectionOSIReferenceModel.htm (last visited Nov. 28, 2014).

[77] Paul Krzyzanowski, *Understanding Autonomous Systems*, RUTGERS (Apr. 5, 2013), https://www.cs.rutgers.edu/~pxk/352/notes/autonomous_systems.html.

[78] *Id.*

[79] *Id.*

[80] Margaret Rouse, *Autonomous System (AS)*, TECHTARGET, http://searchnetworking.techtarget.com/definition/autonomous-system (last visited Nov. 28, 2014).

[81] Krzyzanowski, *supra* note 77.

[82] KUROSE & ROSS, *supra* note 22, at 394.

[83] *Id.* at 374.

[84] *Id.* at 394.

[85] *Id.*

1. Routing Between Networks: Border Gate-way Protocol

The Border Gate-Way Protocol (BGP) is the routing algorithm that governs the inter-AS transfer of data.[86] BGP is extremely complex.[87] Whole books have been written on it and it can take years to master.[88] It provides each AS a means to obtain outside AS reachability information from bordering ASes.[89] The BGP algorithm determines good routes to destinations based on reachability information and on AS policy that is decided by AS administrators.[90]

BGP route selection rules are very complicated. According to BGP, when a router needs to find a path to a destination, it first finds all possible routes to the destination.[91] If more than one route exists to the destination, the router selects a route which is primarily based on policy decisions made by the AS's network administration.[92] If more than one route remains after eliminating all other routes based on policy decisions, then the routes with the shortest paths (the smallest number of router hops) are selected.[93] If more than one route still remains, then the algorithm narrows down routes based on other criteria.[94]

2. Routing Policy

Path finding in BGP is primarily based on policy decisions made by the AS administrator.[95] This makes path finding more complicated. If a router knows of a path from point A through itself to point C, it may not advertise it to other routers due to policy.[96] In this way, it can prevent itself from transferring a packet that the administrator does not want it to transfer.[97] "[F]or example, a rule such as 'router x, belonging to organization y should not forward any packets originating from the network owned by organization Z'" can be implemented by the

[86] *Border Gateway Protocol (BGP)*, TECHOPEDIA, http://www.techopedia.com/definition/6193/border-gateway-protocol-bgp (last visited Dec. 5, 2014).

[87] KUROSE & ROSS, *supra* note 22, at 401.

[88] *Id.*

[89] *BGP*, *supra* note 86.

[90] KUROSE & ROSS, *supra* note 22, at 400.

[91] Ivan Pepelnjak, *BGP Troubleshooting: Advanced Approach*, TECHTARGET, http://searchtelecom.techtarget.com/feature/BGP-essentials-The-protocol-that-makes-the-Internet-work (last visited Dec. 5, 2014).

[92] KUROSE & ROSS, *supra* note 22, at 404.

[93] *Id.* at 405.

[94] *Id.*

[95] *Id.* at 404.

[96] CISCO IOS IP CONFIGURATION GUIDE, RELEASE 12.2, at IPC-372 (2006), *available at* http://www.cisco.com/c/en/us/td/docs/ios/12_2/ip/configuration/guide/fipr_c/1cfindep.html#wp1001343.

[97] KUROSE & ROSS, *supra* note 22, at 404.

administrator of an AS.[98] Policies have developed according to the problems that Internet Service Providers (ISPs) have faced.[99] Two researchers categorized the policies into several groups including (1) policies based on economic relationships an ISP has with its neighboring ISP; (2) policies based on the need to control traffic flow and to avoid overloading routers; and (3) security related policies to protect against cyberattacks.[100]

This discussion on how routes are selected over the internet shows that state borders and territory do not play a role in determining routes. Invariably some data sent over the internet crosses through multiple state borders.[101] Even when two people send data within state A, it is possible that the data travels through state B because BGP does not account for state borders when finding routes.[102] This unique characteristic of the internet allows states to gather and decrypt data from many other states as the data crosses borders. This is important because the law of sovereignty is heavily based on territory and state borders.[103] Sovereignty allows states to take advantage of algorithms that do not account for state borders when transferring data.[104] In the next Part, I will summarize the aspects of sovereignty that apply to gathering data and breaking encryption.

III. SUMMARY OF THE LAW OF SOVEREIGNTY

According to the international legal principle of sovereignty, states have a number of rights that come with a number of obligations.[105] These rights allow states to gather and decrypt data in many instances.[106] Conversely, the obligations given to states through sovereignty describe what types of actions taken while gathering and decrypting data would violate international law.[107]

[98] *Id.* at 374.

[99] Matthew Caesar & Jennifer Rexford, *BGP Routing Policies in ISP Networks*, PRINCETON, http://www.cs.princeton.edu/~jrex/papers/policies.pdf (last visited Nov. 22, 2014).

[100] *Id.*

[101] Eric Jensen, *Cyber Sovereignty: The Way Ahead*, 50 TEX. INT'L L.J. 7 (forthcoming 2015).

[102] *Id.*

[103] *Id.*

[104] *Id.*

[105] *Id.*

[106] *See infra* Part V.

[107] Jensen, *supra* note 101.

A. *Rights and Obligations of Sovereignty*

Sovereignty gives states the right to deal with each other as equals under the law.[108] "The United Nations are based on the principle of sovereign equality of all its members and preserving state sovereignty is a top priority for both international organizations and individual states."[109] States have an equal right to use resources from the global commons.[110] Likewise, when states act, they must take into consideration the rights of other sovereign states especially with regard to the global commons, natural resources, the environment, and events during armed conflicts.[111] A state must take into account other states' interests when it makes decisions[112] and must avoid harming another state's ability to exercise its rights.[113] States are also obligated to solve disputes peacefully.[114]

States have exclusive power over their own territory.[115] Territory includes "land territory, internal waters, territorial sea (including bed and subsoil), archipelagic waters, or national airspace."[116] According to the arbitral decision in *Island of Palmas*, "[s]overeignty in the relations between States signifies independence."[117] "Independence in regard to a portion of the globe is the right to exercise therein, to the exclusion of any other State, the functions of a State."[118] This notion of exclusivity is further confirmed by the International Court of Justice which stated that sovereignty is the "body of rights and attributes which a State possesses in its territory, to the exclusion of all other States."[119] By extension of

[108] JAMES CRAWFORD, BROWNLIE'S PRINCIPLES OF PUBLIC INTERNATIONAL LAW 447 (8th ed. 2012).

[109] Andrew Liaropoulos, *Exercising State Sovereignty in Cyberspace: An International Cyber-Order Under Construction?*, PROCEEDINGS OF THE 8TH INT'L CONF. ON INFORMATION WARFARE AND SECURITY 137–38 (Mar. 2013).

[110] EDITH BROWN WEISS, IN FAIRNESS TO FUTURE GENERATIONS: INTERNATIONAL LAW, COMMON PATRIMONY, AND INTERGENERATIONAL EQUITY 117 (1989).

[111] Jensen, *supra* note 101 (manuscript at 14).

[112] George K. Walker, *Defining Terms in the 1982 UNCLOS Convention IV: The Last Round of Definitions Proposed by the International Law Association (American Branch) Law of the Sea Committee*, 36 CAL. W. INT'L L.J. 174 (2005).

[113] Chinthaka Mendis, *Sovereignty vs. Trans-boundary Environmental Harm: The Evolving International Law Obligations and the Sethusamuduram Ship Channel Project*, at 54–55, United Nations (2006), *available at* http://www.un.org/depts/los/nippon/unnff_programme_home/fellows_pages/fellows_papers/mendis_0607_sri_lanka.pdf.

[114] U.N. Charter art. 2, paras. 3–4, arts. 33–38.

[115] TALLINN MANUAL, *supra* note 13, at 25.

[116] *Id.*

[117] Island of Palmas (Neth. v. United States), 2 R.I.A.A. 829, 838 (Perm. Ct. Arb. 1928).

[118] *Id.*

[119] Corfu Channel (United Kingdom v. Alb.), 1949 I.C.J. 6, 43 (Apr. 9, 1949) (individual opinion of Judge Alvarez).

their right to exclusivity, states have the right to use domestic resources however they see fit.[120]

States have exclusive power over the populations that lives in their territories[121] as well as things located on their territories.[122] Thus, objects that are within a state's territory but not owned by the state are still subject to any laws that the state imposes on those objects.[123] States exercise sovereignty over cyber infrastructure and any activities associated with the infrastructure that is located on their territory.[124] States also exercise exclusive jurisdiction over objects that are not within their territory but have sovereign immunity.[125] Further, each state has the authority to control "access to and egress from its territory" including access for all forms of communication.[126]

There are, however, limitations on a state's exclusivity of power over its territory. Limitations can come from Security Council actions, the law of armed conflict, fundamental human rights, and any area that the state consents to be bound by a treaty.[127]

In addition, territorial sovereignty comes with several obligations. States must respect the territorial sovereignty of other states.[128] This prohibits states from entering a foreign state and asserting their will without permission.[129] States also have a duty to prevent trans-boundary harm.[130] A state may not knowingly allow its territory to be used to harm

[120] Inaamul Haque & Ruxandra Burdescu, *Monterrey Consensus on Financing for Development: Response Sought from International Economic Law*, 27 B.C. INT'L & COMP. L. REV. 219, 249–50 (2004):

> Under customary international law, principles of sovereignty support a state's clear right to regulate commercial activities within its borders. This power is extensive and encompasses such issues as capacity to engage in business, forms of business enterprises, conditions of continuance of a business, and regulations of capital markets as well as those of foreign capital inflows and outflows.

[121] CRAWFORD, *supra* note 108, at 447; Von Heinegg, *supra* note 12, at 124 (referencing S.S. Lotus (Fr. v. Turk.), 1927 P.C.I.J. (ser. A) No. 10, at 18–20 (Sept. 7)); Free Zones of Upper Savoy and Gex (Fr. v. Switz.), 1932 P.C.I.J. (ser. A/B) No. 46, at 166–69 (June 7).

[122] Von Heinegg, *supra* note 12, at 130.

[123] Jensen, *supra* note 101 (manuscript at 20).

[124] TALLINN MANUAL, *supra* note 13, at 16. Cyber infrastructure is defined as "the communications, storage, and computing resources upon which information systems operate." *Id.* at 24.

[125] Von Heinegg, *supra* note 12, at 124.

[126] *Id.*

[127] Jensen, *supra* note 101 (manuscript at 11).

[128] Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. United States), Judgment, 1986 I.C.J. 14, ¶ 202 (June 27).

[129] *Id.*

[130] Corfu Channel (United Kingdom v Alb), 1949 I.C.J. 4, 22 (Apr. 9, 1949).

another state.[131] This duty to prevent harm also applies to cyber infrastructure and activities within its territory or under its exclusive control.[132] Similarly, states are obligated to protect the rights of other states.[133] States should "pass criminal laws, conduct investigation, prosecute attackers, and cooperate with the victim-states of cyberattacks."[134] If a party causes harm from within a state's borders, the state is required to either have had actual knowledge of the harm or be in a position where it should have had knowledge to be held responsible.[135] A possible emerging norm is that states have the obligation to "monitor cyber infrastructure and take proactive measures to prevent harm."[136] Further, states have the right to monitor, maintain, and repair their sea cables.[137] Thus, states that use submarines to tap submarine cables must be careful to not interfere with those rights.

B. *Protections for Diplomatic Communications*

Diplomatic archives and communications are protected under the Vienna Convention on Diplomatic Relations.[138] Diplomatic archives are protected "at all times and wherever they may be."[139] This applies to both situations when there is no armed conflict as well as during armed conflicts.[140] According to the *Tallinn Manual*, "[d]iplomatic archives and communications are protected from cyber operations at all times" regardless of whether the state is part of an armed conflict or not.[141] Protections for diplomatic communications are also based in customary international law as shown by state practice.[142] Protections given to

[131] *Id.*

[132] Jensen, *supra* note 101, manuscript, at 25.

[133] *Id.* manuscript, at 26.

[134] *Id.*

[135] *Id.* manuscript, at 27.

[136] *Id.* manuscript, at 27–28.

[137] *See* R. Beckman, *Submarine Cables –A Critically Important but Neglected Area of the Law of the Sea*, at 2, presented at Indian Society of Int'l Law, 7th Int'l Conference on Legal Regimes of Sea, Air, Space and Antarctica, New Delhi, Jan. 15–17, *available at* http://cil.nus.edu.sg/wp/wpcontent/uploads/2010/01/Beckman-PDF-ISIL-Submarine-Cables-rev-8-Jan-10.pdf.

[138] Vienna Convention, *supra* note 14, art. 60.

[139] *Id.* arts. 33, 35.

[140] *Id.* art. 27(a) ("[T]he receiving State shall, even in case of armed conflict, respect and protect the consular premises, together with the property of the consular post and the consular archives. . . .").

[141] TALLINN MANUAL, *supra* note 13, at 233; *see* Vienna Convention, *supra* note 14, arts. 33, 35; *see also* Tehran Hostages case, ¶¶ 61–62, 77, 86.

[142] *See* S.C. Res. 667, ¶ 1 (Sept. 16, 1990); S.C. Res. 674, ¶ 1 (Oct. 29, 1990) (condemning Iraq's violation of diplomatic premises during its invasion of Kuwait); S.C. Res. 667, ¶ 3 (Sept. 16, 1990) (demanding compliance with consular protections even though Iraq was involved in an international armed conflict).

diplomatic communications include respect for their confidentiality, integrity, and availability.[143] This requires a state to not interfere with their transmission or reception.[144]

In summary, the law of sovereignty provides for a number of rights for states. The rights are heavily based on the state's territory and they allow the state to control the flow of communication into and out of its borders. In addition, states that operate submarine cables on the high seas have the right to monitor and maintain them. Finally, diplomatic communications are protected from cyberattacks at all times.

IV. HOW SOVEREIGNTY APPLIES TO GATHERING DATA AND BREAKING ENCRYPTION GENERALLY

The preceding discussion on sovereignty helps determine whether, given a particular situation, gathering and decrypting data violates another state's sovereignty or not. This section will discuss some principles created by the law of sovereignty that apply to breaking encryption and gathering data.

Diplomatic communications are protected at all times.[145] Thus, a state must be careful not to violate those protections when gathering data. One way a state might go about gathering and decrypting data is as follows: during the process of downloading and decrypting data, a state could make an initial determination that the data might qualify as a diplomatic communication. If such a determination is made, the state could stop decryption and stop using the data until a full legal review is made. It could continue to download the data just in case the full legal review concludes that the data does not qualify as protected. Finally, if a legal analysis concludes that the data is protected, then the state must stop gathering the data and must delete any data it has stored from the protected communication.

Due to the principle of territorial sovereignty, a state can do nearly anything it wants within its own borders.[146] Thus, if the process of downloading the data and decrypting it occurs entirely within a State's territory or on the high seas, then the action does not violate another state's sovereignty. This means that the downloaded data must have been

[143] Terry Chia, *Confidentiality, Integrity, Availability: The Three Components of the CIA Triad*, IT SECURITY COMMUNITY BLOG (Aug. 20, 2012), http://security.blogoverflow.com/2012/08/confidentiality-integrity-availability-the-three-components-of-the-cia-triad/.

[144] TALLINN MANUAL, *supra* note 13, at 24.

[145] *Infra* Part III.B.

[146] *See* Von Heinegg, *supra* note 12, at 126–27; TALLINN MANUAL, *supra* note 13, at 16–18 (discussing principles of sovereignty as they relate to cyber law); U.N. Convention on the Law of the Sea arts. 86, 89, Dec. 10, 1982, 1833 U.N.T.S. 397, *available at* http://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf.

located on a server or traveling through cables or routers within the state's territory or on or under the high seas.[147]

By the extension of sovereign rights, a state may share any data gathered from within its territory with any other state.[148] By sharing the data, neither the sharing state nor the receiving state would be violating another state's sovereignty. One state may even allow another state's personnel to do the gathering and decrypting work on its territory.[149]

For non-state actors, any actions performed would be subject to the domestic law of the state where the action took place.[150] Depending on the state's domestic law, it may be that a crime is committed when a non-state actor downloads and decrypts data traveling on the internet.

One particularly difficult question is whether installing malware on computers in a foreign state violates that state's sovereignty. According to the Tallinn Manual, a cyberoperation against another state violates that state's sovereignty if it causes damage.[151] Downloading data and breaking encryption, however, usually does not cause any physical damage.[152] The Tallinn Manual further states that "[t]he International Group of Experts could achieve no consensus as to whether the placement of malware that causes no physical damage (as with malware used to monitor activities) constitutes a violation of sovereignty."[153] Although there is no firm consensus, installing malware that causes no physical damage might not be a violation of another state's sovereignty because states seem to regularly install malware in other states without any punishment.[154]

[147] *See* Von Heinegg, *supra* note 146; TALLINN MANUAL, *supra* note 13; U.N. Convention on the Law of the Sea, *supra* note 146.

[148] *See* Von Heinegg, *supra* note 146; TALLINN MANUAL, *supra* note 13; U.N. Convention on the Law of the Sea, *supra* note 146.

[149] *NSA Encryption*, PRODUCTS CRYPTO MUSEUM, http://www.cryptomuseum.com/crypto/usa/nsa.htm (last visited Nov. 28, 2014); Von Heinegg, *supra* note 12, at 126–27.

[150] Jessica Howley, *The Non-State Actor and International Law: A Challenge to State Primacy?*, Dialogue e-Journal at 2–3.

[151] TALLINN MANUAL, *supra* note 13, at 24.

[152] *Id.*

[153] *Id.*

[154] *See, e.g.*, Ellen Nakashima, *China Suspected of Breaching U.S. Postal Service Computer Networks*, WASH. POST (Nov. 10, 2014), http://www.washingtonpost.com/blogs/federal-eye/wp/2014/11/10/china-suspected-of-breaching-u-s-postal-service-computer-networks/; Danny Yadron & Siobhan Gorman, *Hacking Trail Leads to Russia, Experts Say*, WALL ST. J. (Oct. 28, 2014), http://online.wsj.com/articles/hacking-trail-leads-to-russia-experts-say-1414468869.

V. HOW THE LAW OF SOVEREIGNTY APPLIES TO SPECIFIC METHODS OF BREAKING ENCRYPTION

Cryptography is often much more secure in theory than in practice.[155] Often many security weaknesses can be found after examining the "context of a specific implementation and the larger system in which it resides."[156] To defeat cryptography, governments and, to a lesser extent, non-state actors have a variety of techniques at their disposal. Some possible techniques include taking advantage of software vulnerabilities to steal the digital keys used to encrypt data; using superfast computing power to break weak encryption; and in the case of state actors, cooperating with companies to circumvent encryption altogether.[157] This section will discuss several methods that can be used to break encryption. After each method, I will apply the legal principles discussed above and discuss when a particular method might violate another state's sovereignty.

A. *Brute Force Attacks*

1. How it Works

One commonly used method is known as brute force.[158] If Eve has a ciphertext she may be able to decrypt it by computing numerous keys and trying each one until she finds one that works.[159] This attack is often used when trying to learn a user's password.[160] After stealing a file containing encrypted passwords, Eve can try encrypting words from a dictionary.[161] If the encryption matches one of the encrypted passwords, then Eve has effectively decrypted the password.[162] If she knows what user the password belonged to then she can gain access to the system.[163] This attack works because people are not willing to memorize very long passwords.[164] Computers have become fast enough to try billions of

[155] STAMP, *supra* note 36, at 218.

[156] *Id.*

[157] Tom Simonite, *NSA Leak Leaves Crypto-Math Intact but Highlights Known Workarounds*, MIT TECH. REV. (Sept. 9, 2013), http://www.technologyreview.com/news/519171/nsa-leak-leaves-crypto-math-intact-but-highlights-known-workarounds/.

[158] Kevin Parrish, *NSA Hasn't Cracked Basic Internet Encryption (Yet)*, BUS. INSIDER (Sept. 6, 2013), http://www.tomsguide.com/us/encryption-nsa-edward-snowden-rsa-ssl,news-17503.html

[159] TECHREPUBLIC, PASSWORD CRACKING/BRUTE-FORCE TOOLS 208 (3d. 2006).

[160] *Id.* at 196.

[161] *Id.*

[162] *Id.* at 208.

[163] *Id.* at 209.

[164] BRUCE SCHNEIER, SCHNEIER ON SECURITY 166 (2008).

passwords per second.[165] Thus, passwords that are common words, or passwords that are too short (usually less than 13 letters) are easy to crack.[166]

The *New York Times* has reported that the NSA uses supercomputers to break encryption.[167] Supercomputers would be well-suited to perform brute force attacks because they can perform a great number of calculations per second. It has been reported that the NSA can "overpower a relatively weak form of encryption used by most websites that offer secure SSL connections."[168] Most sites that use SSL also use the RSA encryption algorithm with keys that are 1024 bits long.[169] However, "experts have cautioned for years that longer keys are needed to defend against an attacker with the resources of a government agency or large company."[170] Google, for example, has switched to using RSA keys that are 2048 bits long.[171] Some cryptographic algorithms are not able to withstand brute force attacks as well as others. For example, due to its weakness against brute force attacks, Microsoft has advised developers to stop using the SHA-1 hash algorithm.[172] If companies were to use larger bit keys like 2048 or 4096 bit keys, then brute force would be much more difficult because it would take computers too long to figure out the correct key.[173]

2. How the Law Applies

Brute force attacks can be performed after the data is gathered or perhaps even as it is being gathered. The attacks only require local computing power and can be performed without using foreign resources or performing computations on foreign soil. Because a state has exclusive power over its own territory, this kind of computing will not violate any

[165] Dan Goodin, *25-GPU Cluster Cracks Every Standard Windows Password in <6 Hours*, ARS TECHNICA, (Dec. 9, 2012), http://arstechnica.com/security/2012/12/25-gpu-cluster-cracks-every-standard-windows-password-in-6-hours/ (discussing a setup that can try 350 billion passwords per second).

[166] *Id.*

[167] Nicole Perlroth et al., *N.S.A. Able to Foil Basic Safeguards of Privacy on Web*, N.Y. TIMES (Sept. 5, 2013), http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?pagewanted=all&_r=0.

[168] Simonite, *supra* note 157.

[169] *Id.*

[170] *Id.* (the longer a key is, the harder it is to crack using brute force).

[171] Michael Mimoso, *How the NSA Could Be Breaking SSL*, THREAT POST (Dec. 4, 2013), http://threatpost.com/how-the-nsa-could-be-breaking-ssl/103091.

[172] *Id.*

[173] *Id.*; Dan Goodin, *SHA1 Crypto Algorithm Underpinning Internet Security Could Fall by 2018*, ARS TECHNICA, Oct. 6, 2012, http://arstechnica.com/security/2012/10/sha1-crypto-algorithm-could-fall-by-2018/.

other state's sovereignty.[174] One potential violation is if the data is gathered in foreign territory such as from an underwater sea cable located in another state's territorial waters.[175] While states do not have sovereign rights over areas on the high seas, they do have sovereign rights over their own territorial waters.[176] Thus, if state B sends a submarine into the territorial waters of state A without permission to gather data from its submarine cables then state B would likely be violating state A's sovereignty. However, in this kind of scenario, assuming the brute force computations were to be performed after the submarine had left the territory of state A, only the crossing into state A's territory to gather data would be a violation.[177] Subsequent brute force computations on the high seas or within state B's territory would not be a violation of sovereignty.[178]

B. *Defeating Cryptography by Obtaining the Key*

1. How it Works

Another method used to defeat encryption is to collect keys that are used for encryption.[179] By taking advantage of software vulnerabilities or social engineering, a hacker can gain full control over a server or computer.[180] Once control is obtained, the hacker can steal any digital keys that are stored on the server.[181] Although this probably does not work well when large numbers of computers need to be infiltrated, it can be very effective against specific targets.[182] States have been reported to gather encryption keys from online services so they can easily decrypt intercepted data.[183] This method of attack works because one particular key may be used over a long period of time.[184] The effectiveness of this

[174] *See* Von Heinegg, *supra* note 146; TALLINN MANUAL, *supra* note 13; U.N. Convention on the Law of the Sea, *supra* note 146.

[175] TALLINN MANUAL, *supra* note 13.

[176] *Id.*

[177] *Id.* at 25.

[178] *NSA Encryption*, *supra* note 149; Von Heinegg, *supra* note 12.

[179] Hiroshi Shinotsuka, *How Attackers Steal Private Keys from Digital Certificates*, SYMANTEC (Feb. 22, 2013), http://www.symantec.com/connect/blogs/how-attackers-steal-private-keys-digital-certificates.

[180] *Id.*

[181] *Id.*

[182] *Id.*; *see also* Matthew Green, *How Does the NSA Break SSL?*, CRYPTOGRAPHY ENGINEERING (Dec. 2, 2013), http://blog.cryptographyengineering.com/2013/12/how-does-nsa-break-ssl.html ("I'm well aware that NSA can install malware on your computer and own any cryptography you choose. That doesn't interest me at all, for the simple reason that it doesn't scale well. NSA can do this to you, but they can't do it for an entire population.").

[183] Simonite, *supra* note 157.

[184] Green, *supra* note 182 ("This issue is of particular concern in servers configured for

attack could be minimized if companies used perfect forward secrecy, a technique in which keys are not reused.[185]

2. How the Law Applies

The legal analysis of this type of attack depends on how the key used for decryption is obtained.[186] Keys are often obtained by exploiting software vulnerabilities on specific targets.[187] Some software vulnerabilities will allow the attacker to install malware on the target computer, enabling the attacker to do anything he or she wants with the computer.[188] The legal conclusion depends heavily on whether installing malware on a foreign computer amounts to a violation of that nation's sovereignty.[189] According to the Tallinn Manual, no consensus was achieved in situations where malware that allowed spying was installed but where no permanent damage to property occurred.[190] Stealing keys from a server would likely not cause permanent damage to property because it involves simply locating the key on the server's memory and sending it over the internet to another computer.[191] Because the law is unclear on whether installing malware to gather cryptographic keys violates sovereignty or not, a conclusion cannot be made in either direction.

C. *Man in the Middle Attacks*

1. How it Works

In a man in the middle attack, "the attacker intercepts messages in a public key exchange and then retransmits them, substituting his own public key for the requested one, so that the two original parties still appear to be communicating with each other."[192] The communications

the TLS RSA handshake, where a single 128-byte server key is all you need to decrypt every past and future connection made from the device.").

[185] Parker Higgins, *Pushing for Perfect Forward Secrecy, an Important Web Privacy Protection*, ELECTRONIC FRONTIER FOUNDATION (Aug. 28, 2013), https://www.eff.org/deeplinks/2013/08/pushing-perfect-forward-secrecy-important-web-privacy-protection; Simonite, *supra* note 157 ("The value of stealing keys can be mostly neutralized if Internet providers adopt a technique called perfect forward secrecy, in which keys aren't reused. So far Google and a few other companies have adopted it.").

[186] Higgins, *supra* note 185.

[187] *Id.*

[188] *Id.*

[189] *Id.*

[190] *See* TALLINN MANUAL, *supra* note 13, at 16–18.

[191] *Id.*

[192] Margaret Rouse, *Man in the Middle Attack (Fire Brigade Attack)*, TECHTARGET, http://searchsecurity.techtarget.com/definition/man-in-the-middle-attack (last visited Nov. 28,

appear to be going directly to the intended party but in reality, the messages are intercepted and can be tampered with before reaching their final destination.[193] It is possible to avoid cryptography altogether with this type of attack.[194] It has been reported that either the GCHQ or NSA uses this method to intercept internet traffic.[195] One of the agencies "appears to have hacked into a target's Internet router and covertly redirected targeted Google traffic using a fake security certificate so it could intercept the information in unencrypted format."[196] Some security bloggers have speculated that this is done with the cooperation of Google and some other companies.[197] Some companies like Google and Microsoft act as their own Certificate Authority.[198] Thus, they would be able to give a third party a certificate and validate it too.[199] The third party would then be able to act as a man in the middle, intercepting traffic that was intended for Google or some other company's website.[200] Using this method, an attacker would be able to read all the traffic for a given SSL session because the attacker has the certificate and all keys associated with the session.[201]

The entire process could work as follows: first a user sends a request to a Google server.[202] A hacked router then reroutes requests from targeted senders to a man in the middle (MITM) server.[203] The MITM server would then be able to read and tamper with the request before forwarding it on to the legitimate Google server.[204] The Google server then sends back the requested information to the MITM server.[205] The MITM server will then have the ability to read and tamper again with the information from Google.[206] Finally, the MITM server forwards the

2014).

[193] *Id.*

[194] *Id.*

[195] Simonite, *supra* note 157.

[196] Ryan Gallagher, *New Snowden Documents Show NSA Deemed Google Networks a "Target*," SLATE (Sept. 9, 2013), http://www.slate.com/blogs/future_tense/2013/09/09/shifting_shadow_stormbrew_flying_pig_new_snowden_documents_show_nsa_deemed.html.

[197] Paul Bauer, *How the NSA Bypasses Online Encryption*, BAUER-POWER, http://www.bauer-power.net/2013/09/how-nsa-bypasses-online-encryption.html#.VGttI8lL82Y (last visited Nov. 28, 2014).

[198] For example, if you go to www.google.com, you can click on the padlock icon that appears next to the URL. Upon clicking, a message appears showing that the certificate is verified by Google Inc.

[199] Gallagher, *supra* note 196.

[200] Bauer, *supra* note 197.

[201] *Id.*

[202] *Id.*

[203] *Id.*

[204] *Id.*

[205] *Id.*

[206] *Id.*

requested information to the original User.[207] Throughout this process the user would be unaware that there is a third party intercepting all of the traffic.[208] Even if this type of attack is not currently being used by any state, it is a possible method for circumventing encryption.[209]

2. How the Law Applies

This type of attack requires (1) hacking into and taking control of a router; and (2) obtaining and using a certificate that has been falsely authenticated by a certificate authority.[210] In other words, the certificate authority authenticates the certificate even though it knows that the party that is using the certificate is not who the user thinks is using the certificate.[211] If the router is located within the state's territory then a state would not violate sovereignty by taking control of the router.[212] Hacking would likely cause no physical damage to the router or anything else because the purpose of the hacking is to reroute the information to another MITM server. Thus, even if the router were located in another state, the hacking might not be a violation of that state's sovereignty. However, there is no consensus on whether such a hack would be a violation of sovereignty.

Obtaining a falsely authenticated certificate would require a state to cooperate with a company that acts as a certificate authority.[213] The company would need to give the state certificates and make sure that the certificates remain certified. This kind of cooperation would not violate another state's sovereignty even if the company is located in a foreign state. One scenario might involve state A cooperating with a company located in state B to obtain certificates. State A could then use those certificates to carry out MITM attacks against state or non-state actors located in state C. State B does not have a duty to prevent the company from handing over authenticated certificates to state A. Any violation of sovereignty would not occur until the certificate is used improperly. State A would likely not be violating state C's sovereignty as long as it is

[207] *Id.*

[208] *Id.*

[209] *Id.*

[210] *Id.*

[211] *Id.*

[212] *Id.*

[213] Although it is possible to steal and use a certificate (similar to what was done with Stuxnet), cooperation would be needed in the long term. As soon as the certificate is discovered to have been stolen, the certificate authority will revoke it and the certificate will no longer be trusted. *See Revoking an SSL Certificate*, GODADDY, https://support.godaddy.com/help/article/4747/revoking-an-ssl-certificate (last visited Dec. 4, 2014). For a discussion on Stuxnet, see Ralph Langner, *To Kill a Centrifuge*, LANGNER (Nov. 2013), *available at* http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf.

simply gathering data for intelligence purposes. It might be possible for state A to violate state C's sovereignty if it were to make substantial changes to the information from state C that is en route to state B. For example, if state A were to change equipment orders so that they were shipped to state A instead of state C then it might be a violation of state C's sovereignty.

Because sovereignty is heavily based on territory, it may be necessary in some situations to track where connections are made (it is possible to track where connections are made[214]). Although it may take extra resources to figure out where connections to foreign servers are made, tracking connections may be necessary to make sure a state is not violating another state's sovereignty.

D. *Take Advantage of Predictable Random Number Generators*

1. How it Works

Random number generators (RNG) play an important part in SSL and have recently come under scrutiny. There is evidence suggesting that RNGs have been compromised by government agencies.[215] However, some experts question whether tampering actually occurred.[216] In this subsection, I will only address sovereignty in relation to taking advantage of a RNG that is known to be predictable. The law applicable to the intentional placement of flaws in RNGs is a separate issue.

In cryptography, random numbers are used in algorithms such as RSA and Diffie-Hellman to make them work properly. Specifically, RNGs are used to generate "RSA key pairs (i.e. randomly selected large primes), and Diffie-Hellman secret exponents."[217] To summarize, the keys used in public key cryptography are created by using RNGs. For cryptography to work properly, the numbers must not only be statistically random, but they must also be unpredictable (there is a difference between random and unpredictable).[218] If RNGs used in the popular encryption methods are compromised, then anyone may be able to predict the keys used in

[214] KUROSE & ROSS, *supra* note 22, at 43 (discussing the Traceroute program that can report the routers that packets travel through back to the user).

[215] *NSA 'Altered Random-Number Generator*,' BBC NEWS (Sept. 11, 2013), http://www.bbc.com/news/technology-24048343 (stating that the NSA had "written a flaw into a random-number generator that would allow the agency to predict the outcome of the algorithm").

[216] Simonite, *supra* note 157 (stating that "the standard, Dual_EC_DRBG, was always too slow to see widespread use. If the flaw was planted by the NSA, it was an unsubtle and poorly targeted plan, says Callas.").

[217] STAMP, *supra* note 36, at 145. RSA and Diffie-Hellman are widely used cryptographic algorithms. *See* Carlos Frederico Cid, *Cryptanalysis of RSA: A Survey* (2003), *available at* http://www.sans.org/reading-room/whitepapers/vpns/cryptanalysis-rsa-survey-1006.

[218] *Id.* at 146.

encryption and decrypt any ciphertext that used the encryption method. For example, assume Eve, Alice, and Bob all have cryptographic keys generated by the same system. With predictable numbers, Alice and Bob might team up and predict the key that Eve is using based on the numbers used in their own keys.[219] The security of the system could be compromised with some collusion and guess work.[220]

Predictable random numbers could be attacked in at least a couple different areas of an SSL session. If RSA is the chosen cryptographic algorithm, a RNG is used on the client side to create the master secret key (Bob, the customer, represented the client side in the SSL explanation in Part II).[221] If Diffie-Hellman is used, both the client and server sides use RNGs because Diffie-Hellman requires a contribution from the client and the server.[222] Similarly, in Diffie-Hellman, if the RNG is predictable then an attacker would be able to decrypt the entire session.[223]

2. How the Law Applies

Taking advantage of a predictable RNG requires (1) some kind of ingenuity by the attacker to predict the key used in the encryption algorithm; and (2) access to the data that is encrypted. As long as the data is obtained without violating another state's sovereignty (*i.e.*, the data is obtained when it is traveling through the state's own territory or on the high seas) then the entire decryption process will not violate sovereignty.

E. *Side Channel Attacks*

1. How it Works

Side channel attacks can also be used to defeat encryption. Side channel attacks require an additional channel of information about the cryptographic system because they do not directly attack the cryptographic algorithm.[224] The additional channel of information may come from measurements of the time it takes to encrypt a message,

[219] *Id*.

[220] *See* Brad Arkin et al., *How We Learned to Cheat at Online Poker: A Study in Software Security*, CIGITAL (Sept. 1999), http://www.cigital.com/papers/download/developer_gambling.php (detailing how an online Texas Hold'em game was exploited due to the improper implementation of a pseudo-random number generator); Dan Kaminsky, *Primal Fear: Demuddling the Broken Moduli Bug*, DAN KAMINSKY'S BLOG (Feb. 17, 2012), http://dankaminsky.com/2012/02/17/primalfear/ (explaining how RSA can be undermined by predictable number generators).

[221] Green, *supra* note 182.

[222] *Id.*

[223] *Id.*

[224] STAMP, *supra* note 36, at 210-11; FERGUSON ET AL., *supra* note 28, at 132–33.

magnetic fields surrounding the system, radio frequency emissions from the system, and power consumption during the encryption or decryption process.[225] By gathering information from these other channels, an attacker may be able to infer something about the key or the message involved.[226]

Recently, researchers discovered how to break 4096-bit RSA by listening to a computer with a microphone.[227] The researchers recorded the high-pitched (10 to 150 KHz) sounds that are created when the computer decrypts data.[228] The sound is created by "the CPU's voltage regulator, as it tries to maintain a constant voltage during wildly varied and bursty loads."[229] The researchers were able to discover the key that was used from the sounds created, allowing them to decrypt any message that is encrypted with that key.[230] This technique would allow an attacker to obtain a decryption key by placing his phone near a computer and recording the sound that is made.[231] An attacker could also install malware on a target's phone (through spear phishing or some other method) and then remotely record the sound made by any computers decrypting activities that the target has access to.[232] Attackers could also build websites that listen to a computer's CPU when a target visits the website because code used in websites (such as HTML5 and Flash) has microphone access capabilities.[233] The researchers also mentioned that it may be possible to place a microphone in an area where many servers are located to obtain the keys used by the servers.[234]

The sound is created by "the CPU's voltage regulator, as it tries to maintain a constant voltage during wildly varied and bursty loads."[235] The researchers were able to discover the key that was used from the sounds created, allowing them to decrypt any message that is encrypted with that key.[236] This technique would allow an attacker to obtain a decryption key by placing his phone near a computer and recording the

[225] Ferguson et al., *supra* note 28, at 132–33.

[226] *Id.*

[227] Sebastian Anthony, *Researchers Crack the World's Toughest Encryption by Listening to the Tiny Sounds Made by Your Computer's CPU*, ExtremeTech (Dec. 18, 2013), http://www.extremetech.com/extreme/173108-researchers-crack-the-worlds-toughest-encryption-by-listening-to-the-tiny-sounds-made-by-your-computers-cpu.

[228] *Id.*

[229] *Id.*

[230] *Id.*

[231] *Id.*

[232] *Id.*

[233] *Id.*

[234] *Id.*

[235] *Id.*

[236] *Id.*

sound that is made.[237] An attacker could also install malware on a target's phone (through spear phishing or some other method) and then remotely record the sound made by any computers decrypting activities that the target has access to.[238] Attackers could also build websites that listen to a computer's CPU when a target visits the website because code used in websites (such as HTML5 and Flash) has microphone access capabilities.[239] The researchers also mentioned that it may be possible to place a microphone in an area where many servers are located to obtain the keys used by the servers.[240]

2. How the Law Applies

If the target computer is physically located within the territory of the state that is using a side-channel attack then the attack does not violate sovereignty.[241] Domestic law would be required to prevent a state from using such an attack. If a website or a user's computer is hacked, there is no strong legal conclusion whether installing malware on a computer is a violation of sovereignty. If a state places a listening microphone in a server room in another country without permission then this is more likely a violation of sovereignty. Placing a microphone in a foreign country requires a state actor to enter the territory of another state and interfere within the foreign state's borders.[242]

F. *Submarine Tapping*

1. How it Works

Submarine tapping may be a useful technique in gaining access to data that might not otherwise enter a state's territory. If the tapping occurs on the high seas, then no state can claim sovereignty over the location where the tapping occurs. In 2005, the Associated Press reported that a submarine, the USS Jimmy Carter, had been modified to carry crews of technicians to tap fiber optic lines on the seabed.[243] It is easiest to tap the cables at the locations where the cables' signals are amplified allowing them to travel long distances.[244] They are easier to tap at these locations

[237] *Id*.

[238] *Id*.

[239] *Id*.

[240] *Id*.

[241] *See* Von Heinegg, *supra* note 12, at 126.

[242] *Id*.

[243] *New Nuclear Sub is said to have Special Eavesdropping Ability*, N.Y. TIMES (Feb. 20, 2005), http://www.nytimes.com/2005/02/20/politics/20submarine.html.

[244] Fabian Schmidt, *Tapping the World's Fiber Optic Cables*, DEUTSCHE WELLE (June 6, 2013), http://www.dw.de/tapping-the-worlds-fiber-optic-cables/a-16916476.

because each wire is treated individually instead of in a bundle.[245] However, submarine tapping may only be necessary for cables that are not reachable through any ally state. If a state has access to locations where the cables make landfall, then it will likely tap the cable on land because it is easier.[246]

2. How the Law Applies

Whether submarine cable tapping violates sovereignty depends on where the tapping occurs and what kind of technique is used to tap the cables. To avoid violating another state's sovereignty the tapping must occur within the tapping state's territorial waters or on the high seas.[247] The technique used must be one that does not damage the cable or interfere with the cable operating state's right to right to monitor, maintain, and repair its submarine cables.[248] Thus, the tapping must not cause damage to the submarine cables and must not prevent the data traveling through them from reaching its destination.

VI. CONCLUSION

Sovereignty gives states the right to intercept and decrypt data inside their territory or on the high seas. There are several methods that can be used to break cryptography. Whether the method violates another state's sovereignty often depends on where physical actions take place and whether the cyber infrastructure that is being attacked is located on another state's territory. However, it is unclear whether defeating encryption by attacking computers in foreign states violates sovereignty or not. Finally, states must be careful of protections for diplomatic communications as they gather and decrypt data.

[245] *Id*.

[246] Olga Khazan, *The Creepy, Long-Standing Practice of Undersea Cable Tapping*, ATLANTIC (July 16, 2013), http://www.theatlantic.com/international/archive/2013/07/the-creepy-long-standing-practice-of-undersea-cable-tapping/277855/.

[247] *See* Von Heinegg, *supra* note 12, at 127.

[248] *See* Vienna Convention, *supra* note 14.