Journal of Military and Strategic Studies, Fall 2005, Vol. 8, Issue 1.

# STATE AUTONOMY AND ENCRYPTION: AN EXAMINATION OF TECHNOLOGY'S ABILITY TO IMPACT STATE AUTONOMY

***Nathan Klassen, MA student, Department of Political Science, University of Regina***

Dialogue surrounding the impact of technology upon the state is frequently framed as a conflict between technology and sovereignty. Traditionally these discussions have been placed within the context of the larger debate surrounding globalization. This has typically limited the discussion of technology and its impact upon sovereignty to advances in telecommunications and the resulting impact these have had on the global financial community.[1] This framing is understandable and perhaps justified due to the supra-geographic nature of communications technology which appears to challenge the territorial nature of state sovereignty. However, technology can be used in a variety of ways. It may challenge the state and its roles, but it also has the potential to strengthen the state. In actuality it is not sovereignty itself that is being challenged, but state autonomy. Sovereignty is an absolute concept and certainly autonomy is a component of sovereignty. However, discussion surrounding sovereignty is theoretical and quickly degenerates into a comparison of definitions rather than an assessment of impact. This paper will examine the impact of technology upon state autonomy, and more specifically how technology threatens state autonomy. Under close examination here is the policy debate surrounding a single technology, encryption.

Due to the complexity of the issues presented within this paper, it is important

[1] Saskia Sassen, *Losing Control? Sovereignty in an Age of Globalization* (New York, NY: Columbia University Press, 1996), Susan Strange, *Mad Money: When Markets Outgrow Governments* (Manchester, MI: University of Michigan Press, 1998) and Susan Strange, *The Retreat of the State: The Diffusion of Power in the World Economy* (Cambridge, UK: Cambridge University Press, 1996).

that the fundamental concepts are well understood. This paper begins by developing a framework of analysis by examining state autonomy and sovereignty which will be employed to determine the impact technology may have upon state autonomy. Once the framework has been introduced, the paper will turn to an introduction of encryption. Cryptography, the study of encryption, is a complex field. This author has made a sincere effort to make this discussion accessible. This will result in oversimplification for individuals well-versed in the field, but increase accessibility for those who are not. The discussion will focus on the role of encryption within national security and its impact on the information gathering process. The paper will introduce the challenges surrounding cryptanalysis and pursue a case study of two encryption policy options, key escrow and export controls, explored by the United States. The conclusion will integrate the case study into the theoretical framework and answer the question of whether or not encryption challenges state autonomy.

## State Autonomy

In order to discuss state autonomy, we must first define the concepts of sovereignty, the state, and autonomy. “Sovereignty is the claim to be the ultimate political authority, subject to no higher power as regards the making and enforcing of political decisions.”[2] The powers of sovereignty are normally vested within the institution of the state. The state can be defined as a "distinct set of political institutions whose specific concern is with the organization of domination, in the name of the common interest, within a delimited territory."[3] The state's goal is to exercise

[2] Ian McLean and Alistair McMillan, *Oxford Concise Dictionary of Politics* (Toronto, ON: Oxford University Press, 2003), p. 502.
[3] Ibid., p. 512.

sovereignty, absolute power within a specific territory, whereby the state's actions within that territory are autonomous. Autonomy is "the ability of states to pursue goals in spite of the demands or interests of other social groups or classes."[4] This series of definitions presents autonomy as an implied component of sovereignty, and indeed the two are linked. A clear articulation of this link can be found within the Westphalian state:

The Westphalian state is a system of political authority based on territory and autonomy. Territoriality means that political authority is exercised over a defined geographic space, rather than, for instance, over people, as would be the case in a tribal form of political order. Autonomy means that no external actor enjoys authority within the borders of the state.[5]

By definition, the Westphalian state is a sovereign state, for only a sovereign can operate with autonomy. This articulation leaves no doubt that autonomy is one of the key concepts of not only the Westphalian notion of sovereignty but of sovereignty in general. Yet the discussion so far has an important problem: sovereignty, territoriality and autonomy are all defined as absolutes.

Stephen Krasner provides an insightful critique of the Westphalian notion of sovereignty.[6] He argues that states have been willing to set aside, or cling to, the notion of Westphalian sovereignty in order to secure benefit when opportunity arises. States which take actions that result in benefit do so voluntarily. States that are the victims of actions, those that result in them receiving no benefit, do so involuntarily. Krasner provides a detailed historical analysis of state actions to support his claim. He concludes:

[4] Ibid., p.460.

[5] Stephen D. Krasner, "Compromising Westphalia," *International Security* 20/3: pp. 20, 115-116.

[6] Krasner, "Compromising Westphalia," pp. 115-116.

> In the contemporary world, peace and stability would be better served by explicitly recognizing that the Westphalian model has, in fact and in theory, always been contested. It is historically myopic to take the Westphalian model as a benchmark that accurately describes some golden age when all states exercised exclusive authority within their own borders. Weaker states have frequently been subject to coercion and imposition and been unable to defend their autonomy. Stronger ones have entered into conventions and contracts that violate their autonomy and even territoriality.[7]

If historically both strong and weak states have endured violations of their autonomy, it is impossible for autonomy to be absolute. Therefore, autonomy can only be absolute from a theoretical perspective, not a practical perspective. If absolute autonomy is not possible, then an alternate conception of autonomy is required for analysis. To construct this alternate conception, we must begin by further exploring the state and understanding its responsibilities.

States are not created equal.[8] Different states make use of different systems, exist in different parts of the world, have differently skilled populations, have access to different kinds of resources, are of different ages, and are stable and unstable to varying degrees. Autonomy reflects the degree of control a state exerts over its territory in order to achieve its goals. The degree of autonomy a state is able to exercise is a reflection of the strength, or power, of that particular state. Stronger states will be better able to implement their interests and therefore possess a high degree of autonomy. The fundamental difference between states is the amount of resources they possess and the ability to utilize those resources. All states attempt to implement a common set of functions. The degree to which a state can implement these functions is determined by that state's resources, as these functions clearly dictate state goals. States better able

[7] Ibid., p. 150.

[8] Joseph S. Nye, Jr., *Power in the Global Information Age* (London, UK: Routledge, 2004). Nye states that "the power of states varies as well, as does the significance of nonstate actors in different spheres" (72).

to utilize these resources, and those with greater resources, are better able to achieve their goals. By examining the individual functions it should be possible to examine the degree of autonomy states exercise with regards to specific functions.

There are four primary functions of the state:

1) (to exercise a) monopoly of civil force, i.e., maintaining law and order and national security

2) rule-making, the provision of laws and their judicial application through which a country governs itself

3) direction and regulation of a country's economy

4) providing consciousness of common politico-social identity.[9]

This paper will refer to these four functions as the national security, judicial, economic, and socio-political functions, respectively. States attempt to maximize their autonomy with regards to each individual function. It must be recognized that each of these responsibilities is interdependent.[10] For example, a state incapable of maintaining law and order is not able to fulfil its rule-making obligation. It may make the rules but it is not capable of enforcing them. If the state cannot enforce its rules, it becomes unable to direct or regulate the economy. It is possible that the resulting chaos and lawlessness will result in the dissolution of the common socio-political identity. If this breakdown were to occur the state may become vulnerable to outside intervention or internal conflict. The state would no longer be autonomous in any sense of the word. National security and the maintenance of law and order are required for a state to

[9] Richard Lee Hough, *The Nation-States Concert of Chaos* (Toronto, ON: University Press of America, 2003), p. 23.
[10] Ibid.

remain autonomous and therefore fulfil its primary functions. The interdependence of state responsibilities ensures that as states attempt to exert their autonomy over individual functions they actually assert their autonomy over them all.

Since autonomy is not absolute, let us refer to the point where an individual state exerts the maximum possible degree of autonomy over its functions as potential autonomy. States attempt to pursue a high degree of autonomy, maximizing their potential autonomy, to ensure successful implementation of their functions. Potential autonomy varies from state to state in accordance with their resources and goals, and it can never equal or exceed the theoretical level of absolute autonomy. The ability of a state to implement individual functions autonomously will be referred to as functional autonomy. The functions of the state are broad. Implementation of each function requires the state to address the many subset situations that compose the larger function. The ability of the state to implement individual situations, which are subsets of state functions, is referred to as situational autonomy.

From this discussion, a hierarchy of state autonomy becomes visible. At the highest level, we have the theoretically possible but practically unattainable absolute autonomy. The next level is potential autonomy. States attempt to achieve their potential autonomy through maximum utilization of resources. Therefore, potential autonomy varies between states because state resources vary. Functional autonomy is a level below potential autonomy and reflects a state's ability to implement its functions. The sum of situational autonomy equals the level of functional autonomy for that given function. The sum of functional autonomy, for all four functions, equals the potential autonomy of the state. In practice, potential autonomy is a very difficult point for states to reach and is a point that shifts based upon technological advances and changes in the amount of available state resources.

Detailing technology's impact on state autonomy requires multiple steps. First we must demonstrate that technology can impact situational autonomy. Next we must prove that this impact extends to the functional level. Finally, it must be determined if the functional impact is sufficient to truly effect the potential autonomy of the state. Within this paper, the specific situation analyzed is the information gathering process, a subset under the national security function, and the impact that encryption has upon it. The case study examines the United States as the state with the greatest amount of resources to address this specific challenge.[11] If the United States were to encounter a reduction in potential autonomy due to the impact of encryption upon the information gathering process, this impact would be common to other all states since they have fewer resources to address this challenge. Therefore, our analysis must begin at the situational level with a discussion of significance. Since no state can be perfectly autonomous, we must determine if the failure of a state to exert situational autonomy is significant or not. The failure of a state to exert situational autonomy over an important situation creates a significant impact, therefore it must be demonstrated that an individual situation is important. Important situations will impact the function they are a subset of.

The question then emerges of what qualifies as an important situation. It will be helpful to examine arguments put forward by Susan Strange and Saskia Sassen, both of whom attempt to prove that overall state sovereignty is being reduced.[12] Neither

[11] The specific resources are presented in the cryptanalysis portion of this paper.
[12] Sassen, *Losing Control?*, and Strange, *The Retreat of the State*.

author uses the term situational autonomy, but their analysis of specific situations to prove an impact upon state sovereignty correlates to how various situations may impact state autonomy. Sassen's focus is upon the shift in immigration policy that has occurred as a result of global economic pressures. She believes that a shift in immigration policy focus, from unskilled to skilled labour, is directly linked to global economic influence and therefore constitutes a reduction in state sovereignty.[13] Strange focuses upon how the telecommunications revolution and international trade have reduced the role and power of the state over time. She believes that the telecommunications revolution has impeded the ability for states to censor specific information and that this, among other things, has resulted in a reduction of state power and therefore sovereignty.[14] Strange believes that the reduction of state autonomy is intrinsically linked to technological development. She states that the "accelerating pace of technological change [is] a prime case of the shift in the state-market balance of power."[15] Strange concludes that:

> On some issues, and in some circumstances, state authority will be given priority. On other issues, and in other circumstances, it will not. To say this is not the same as saying the state as an institution is disappearing, that it is on the way out, or that it is being ousted by the multinationals or any other kind of authority. It is only saying that it is undergoing a metamorphosis brought on by structural change in world society and economy...it is becoming, once more and as in the past, just one source of authority among several, with limited powers and resources.[16]

Neither author goes so far as to say the state no longer matters as a unit of analysis, but both imply that its importance will progressively decrease over time as

[13] Sassen, *Losing Control?,* p. 88.
[14] Strange, *The Retreat of the State*, p. 100.
[15] Ibid., p. 7.
[16] Ibid., pp. 72-73.

challenges continue to appear. Within these works is an underlying assumption that the state is unable to adapt to these challenges and that these issues challenge state autonomy. Further, neither demonstrate that a strong state is unable to pursue its potential autonomy, only that it cannot achieve absolute autonomy.

Viewing sovereignty as an absolute concept, it is clear why both Strange and Sassen feel the sovereignty of the state is challenged. If sovereignty is absolute, these authors demonstrate that sovereignty is being eroded, but sovereignty is not absolute. The framework constructed within this paper would describe this as an altering of the functions of the state, as a specific situation is removed from the function. Let us use the example of a function composed of three situations. Situations are binary variable, a zero representing the state not exerting autonomy and a one representing the exertion of state autonomy. A state exerting autonomy over one-hundred percent of its situations would look like: $\frac{1+1+1}{3} = \frac{3}{3}$. If, through voluntary choice, one of these situations is no longer a responsibility of the state: $\frac{1+1}{2} = \frac{2}{2}$. The state still exerts autonomy over one-hundred percent of the situations it wishes to control. However, if the removal of a subset responsibility is not voluntary: $\frac{0+1+1}{3} = \frac{2}{3}$, the state is only exerting autonomy over sixty-six percent of the situations it wishes to control and therefore an impact upon functional and potential autonomy exists. If Strange and Sassen had employed this framework in their analysis, they would have succeeded in demonstrating that the composition of individual state functions changes, not that state autonomy or sovereignty is reduced. There is no impact upon potential autonomy if states voluntarily cede autonomy over a situation.

For purposes of analysis, we must work from the bottom of the hierarchy to the top. For an impact upon situational autonomy to exist it must be proven that the state does not voluntarily cede autonomy for that particular situation. This can include situations where either the state is unable to exert autonomy and wishes to do so or that it has been involuntarily removed from the state's authority. It must also be proven that the situation is important and therefore able to significantly impact the function it falls under. If a state fails to exert autonomy over an important situation, which is by definition significant, a reduction in functional autonomy and therefore potential autonomy will occur, since potential autonomy is the sum of functional autonomy. This case study will demonstrate that information gathering is an important situation and that encryption is significantly reducing the ability of states to exert autonomy over this situation, thereby being capable of reducing state autonomy.

## Cryptography and Encryption

Cryptography is the mathematical field that studies encryption and decryption. It is a highly technical and complicated field. Encryption is the process that converts information in plaintext into the unreadable ciphertext. This process is reversible, as the ciphertext is decrypted back into plaintext with a key.[17] Only the intended key-holding recipient may read the message in its original form. Encryption is not new; the ancient Egyptians were using encryption as early as 2000 BCE.[18] The primary historical use of encryption has been to secure military and political communications, secure

[17] Deborah Russel and G.T. Gangemi, Sr., "Encryption," in *Building in Big Brother: The Cryptographic Policy Debate*, Lance J. Hoffman, ed. (New York, NY: Springer-Verlag Publishers, 1995), pp. 10-14. Russel and Gangemi claim "the key is a kind of password, usually known only to the sender and the recipient of encrypted information."

[18] Ibid., p. 11.

communications being vital to a successful war effort. If an enemy can intercept and understand one's communications, the element of surprise and perhaps the war has been lost.

During the First World War, radio communications were often broadcast unencrypted and were easily intercepted by opposing forces. Realizing their error, states began encrypting their communications but most were unprepared to counter this new mathematical challenge. This lesson was well learned by the outbreak of World War II as both the Axis and Allies struggled to understand each other's transmissions in order to secure a strategic advantage. Japanese codes were eventually broken by the United States, resulting in the American naval victories at Coral Sea and Midway.[19] It could be reasonably argued that successful Allied cryptanalysis[20] made a significant difference in the war. The importance of encryption in providing security during wartime has not been forgotten and has undoubtedly influenced the course of encryption policy since World War II.

Encryption is able to ensure the confidentiality, integrity and authenticity of data. The very nature of encryption ensures that even if data has become physically compromised, it will be very difficult for that data to be read. The integrity function of encryption ensures that the confidential data has not been tampered with intentionally or otherwise. For financial transactions or electronic voting, it is very important that the original data is confidential and that it can be proven to have not been tampered with at any point along the way. Authenticity is slightly different than integrity. Many encryption

[19] Walter B. Wriston, *The Twilight of Sovereignty: How the Information Revolution Is Transforming Our World* (New York, NY: Macmillan Publishing Company, 1992), p. 157.

[20] Cryptanalysis refers to "the process of trying to decrypt encrypted information without the key." Russel and Gangemi, "Encryption," p. 15.

algorithms[21] will be able to authenticate who sent the original information. This coupled with integrity and confidentiality ensures that the received information has not been compromised or altered and has been sent by a trusted actor.[22] These functions have become increasingly important in a society ever more reliant upon information technology. The result is a shift in the use of encryption from solely a military technology to a military/civilian or dual use technology.

This shift is the result of advances in computing technology that have made encryption technology much easier to implement. Encryption has become an important part of modern communications and daily life. Online banking transactions are secured through encryption, as are retail purchases using debit or credit cards.[23] Corporations will often encrypt their data as they share information between various global branches to ensure that the information cannot be read by their competitors. There are countless other examples; clearly, the world has come to rely on encryption to secure sensitive information.

As important as encryption has become it is important to understand that not all encryption algorithms are created equal. Some are strong and some are weak. "The strength of an encryption key is determined by how difficult it would be for a third party to break the code, which depends on the key length, measured in bits, and the complexity of the algorithm in question."[24] These two factors, key length and the algorithm itself, are the primary determinants of strength for they relate directly to the

[21] Encryption algorithms are "the technique or rules selected for encryption (that) determine how simple or how complex the process of transformation will be. Most encryption techniques utilize rather simple mathematical formulas that are applied a number of times in different combinations." Russel and Gangemi, p. 14.

[22] Ibid.

[23] T.H. Bell, M. Fellows, Thimbleby, I. Witten, N. Koblitz and M. Powell, "Explaining Cryptographic Systems," *Computers and Education* 40/3 (2003): p. 200.

[24] Tricia E. Black, "Taking Account of the World As It Will Be: The Shifting Course of US Encryption Policy," *Federal Communications Law Journal* 53/2 (2001): pp. 53, 294-295.

two methods used to break encryption, the brute force and shortcut approaches.[25] The brute force approach generates and tests every possible key value in an attempt to find the one which will decrypt the data. For example, the previous United States government encryption standard, the Digital Encryption Standard (DES), was a 56-bit system at its introduction. The number of keys in a 56-bit system is 2 to the power of 56 or approximately 72 quadrillion possible key values. The more key values there are to test, the longer it will take to break the encryption scheme using a brute force approach. Conversely, the shortcut approach exploits a flaw in the underlying algorithm. The algorithm determines how the key is generated and if the cryptanalyst understands the algorithm and how the key is generated, it may make encryption which employs that algorithm easier to crack. For example, only "recently...nineteen years after DES was introduced have any [short cut attacks] threatened the security of the algorithm."[26] It would appear then that up until this point, any attempts to crack the algorithm would require the brute force approach. Cryptography, being a field of mathematics, uses the principle of peer review, so information regarding encryption algorithms is publicly available to the cryptographic community via academic journals and conferences. The process of peer review will generally uncover any weaknesses within the algorithm. Users of encryption products observe this process and will not use encryption that is known to be weak.

## Information and National Security

Information is fundamentally important to the implementation of the national

[25] Ernest Brickell, Dorothy Denning, Stephen Kent, David Maher and Walter Tuchman, "Skipjack Review: Interim Report," in *Building in Big Brother*, pp. 122-130.

[26] Susan Landau, et al., "Cryptography in Public: A Brief History," in *Building in Big Brother*, p. 42.

security function. All actors involved in national security efforts require information to make decisions and act. Of primary interest to this discussion is the information gathering process. Information gathering is a two-part process involving sorting and synthesis. Sorting refers to the choosing of which information to acquire and then prioritizing the acquired information appropriately. Synthesis is the process of analysing the sorted information and then transmitting it to the appropriate party for decision making. Any impediment to either part of the information gathering process will increase the acquisition cost of the desired information. There are two primary impediments to information gathering: the amount of available information and timely access to information:

> One of the most interesting aspects of power in relation to increasing flows of information is the 'paradox of plenty.' A plentitude of information leads to a poverty of attention. When we are overwhelmed with the volume of information confronting us, it is hard to know what to focus on. ...Unlike asymmetrical interdependence in trade where power goes to those who can afford to hold back or break trade ties, power in information flows goes to those who can edit and authoritatively validate information, sorting out what is both correct and important.[27]

Joseph Nye suggests three categories of information: flows, competitive and strategic. Each successive tier of information will be of a diminishing quantity and increasing importance. The more important the information, the more likely that information is to be protected. In this digital world, that implies the use of encryption. Information flows are publicly available information such as statistics or general news. This information is readily accessible, but its vast quantities pose a significant sorting

[27] Nye, *Power in the Global Information Age*, p. 89.

and synthesis challenge. Competitive information could be characterized as private information flows. This information is more difficult to acquire, but the comparatively lower volume of information allows for easier sorting and synthesis. Strategic information is scarce and very difficult to access.[28] Strategic information is the tier of information most useful to the state for the implementation of the national security function. While strategic information is scarce, it may exist within a vast pool of data, a proverbial needle in the haystack:

> Foreign access to cryptography of even moderate strength poses a problem for US intelligence. Those who think about vulnerabilities from the viewpoint of security typically regard strong encryption of each message as the only barrier to communications intelligence. However, a message cannot be analyzed until it has been located. Locating the traffic of interest is as important a problem as any. Even encryption that is too weak to resist concerted attack can multiply the cost of targeting traffic several-fold.[29]

Given the volume of information and the likelihood that strategic information will be encrypted, encryption appears to challenge the ability of the state to gather information, which may result in a challenge to situational autonomy. There are two options for states to get over the hurdles encryption places in the information gathering process, cryptanalysis and cryptography policy.

## Cryptanalysis

If the problem is not being able to read encrypted information, the solution is to

[28] Ibid.
[29] Landau et al., "Cryptography in Public," p. 119.

find a way to read the encrypted information, even without the key. That process is known as cryptanalysis. It must be emphasized that it is not enough to read the encrypted information - it must be also be read in a timely fashion. Issues of national security constitute strategic information and much of this information may be time sensitive. If a target arranges to meet a contact at a certain time via an encrypted message and the message is intercepted and decoded even hours after the meeting takes place, it is too late. Successful and timely cryptanalysis requires both computing and human resources. Human resources are, of course, the actual human capital of computer scientists, cryptographers and mathematicians, for example, that are required to do the cryptanalysis. Computing resources are the tools employed by this human capital. Significant economic resources are required to develop both of these capacities.

Computing power is the second vital component of cryptanalysis. As computing power increases, the cost of a brute force approach is reduced. During the 1990s, developers at RSA Laboratories created an encryption algorithm that would compete with the DES standard and sponsored a series of challenges to prove that DES was not as secure as believed.[30] The first challenge resulted in a group cracking DES in 90 days. The second challenge was attempted by two separate groups, Distributed.net and the Electronic Frontier Foundation (EFF), who in 1998 broke DES in 39 days and 56 hours respectively.[31] Distributed.net developed a framework that connected thousands of ordinary computers via the internet to work together to crack DES. The EFF pursued a different approach and custom built a computer called Deep Crack.

[30] RSA Laboratories, "DES Challenge III," 1999. Available from http://www.rsasecurity.com/rsalabs/node.asp?id=2108.

[31] The Electronic Frontier Foundation, "DES Cracker Project," 1998. Available from http://www.eff.org/Privacy/Crypto/Crypto_misc/DESCracker/.

Deep Crack was able to test an amazing 88 billion keys a second and was built for less than $250,000.[32] The EFF and Distributed.Net co-operated for the third challenge and broke 128-bit DES encryption in 22 hours. [33] This demonstration proved that DES was not as secure as had been argued and, partially in response to this demonstration, the United States moved to replace the DES with the Advanced Encryption Standard (AES).

DES was not discovered to be insecure through a shortcut attack (although this was eventually done) but rather through the advancement of computing technology, the implication being that as long as computing technology advances, states or groups who wish to break encryption will be able to. This is fundamentally true, but not practically true. Computers will continue to advance, but encryption technology is not stagnant. New algorithms will be designed to address advances in computing power. DES had been around for almost twenty years before it could be swiftly cracked. Finally in the 1990s it was possible for the EFF to design a custom cracking mechanism, which worked incredibly fast due to publicly available knowledge regarding the DES algorithm and advances in computing manufacturing. Additionally, the key size of DES was not large enough to mitigate the challenge of computing technology at the time. Prior to the 1990s, this was not an issue. Current encryption algorithms allow for bit sizes in the thousands, so if a fundamental weakness in that algorithm does not emerge, it will not be possible to break that encryption in a reasonable period of time.

The fundamental challenge with cryptanalysis and national security is that information must be decoded in a timely manner. Let us assume that machines

[32] The Electronic Frontier Foundation, "EFF DES Cracker Machine Brings Honesty to Crypto Debate," 1998. Available from http://www.eff.org/Privacy/Crypto/Crypto_misc/DESCracker/HTML/19980716_eff_descracker_pressrel.html.

[33] The Electronic Frontier Foundation, "RSA Code-Breaking Contest Won Again By Distributed.net and Electronic Frontier Foundation," 1999. Available from http://www.eff.org/Privacy/Crypto/Crypto_misc/DESCracker/HTML/19990119_deschallenge3.html.

equivalent to Deep Crack's functionality exist for every encryption algorithm, and that for approximately $250,000 USD, it would be possible to build a machine capable of decrypting a single message within a 24 to 48 hour time period. Even with this level of functionality, which is unlikely to currently exist, there is a bottleneck. What if there are hundreds of messages to decrypt and only dozens of machines? The sorting portion of the information gathering process becomes very important. If the wrong messages are decrypted or decryption of the vital messages is delayed, the synthesis process is delayed. If a message is intercepted and successfully prioritized for decryption within a 24 hour timeframe but the information details a terrorist attack that will occur 8 hours after the message was intercepted, that information is essentially useless. Individuals who wish to secure their information will determine how long it needs to remain secure. For a terrorist, it may not have to be secure for years, only days or months. They do not have to employ the strongest encryption in existence, only encryption strong enough to prevent timely decryption. Therefore, cryptanalysis alone is not sufficient to mitigate the restriction that encryption places upon the information gathering process and the national security function itself.

## Cryptography Policy

The United States has correctly determined that cryptanalysis is an important part of the national security function but stipulated that it must be supported with effective policy to minimize encryption's impact upon the national security function. Two primary policy options are explored here, key escrow and export controls. Both policies will be viewed through the lens of a specific information gathering situation, wiretapping.

As previously stated, information gathering is fundamental to the insurance of national security and wiretapping is one of the most important information gathering tools available to the intelligence and law enforcement community. Wiretapping can provide credible and timely access to very specific information. It is widely known that wiretapping is used by domestic law enforcement, but it is also employed abroad for foreign intelligence gathering initiatives:

> The government's justification for tight regulation [of encryption] stems from national security concerns. In the past, electronic surveillance, such as court-ordered wiretaps, has proven successful in the detection, prevention, and prosecution of crimes. Based on this success, the government has attempted to limit the overall strength of encryption software so that, when an encrypted message is intercepted, the government will have the ability to decrypt it.[34]

As encryption is increasingly easy to implement, criminals are increasingly likely to encrypt their communications. The type of information gathered by wiretaps is strategic, the tier of information most valued. If cryptanalysis is unable to guarantee timely access to this encrypted information, what option exists for the state? An option explored by the United States during the Clinton administration is known as key escrow. "Key escrow systems are those where part or all of the keys are kept 'in escrow' by third parties. The keys are released only upon proper authority to allow some person other than the original sender or receiver to read the message."[35]

An example will illustrate how key escrow works and what it does. Let us say that Person A and Person B are conducting illicit practices and securing their communications through the use of encryption. As long as their keys remain secure and they employ sufficiently strong encryption, their communications are secure. Let us

[34] Black, "Taking Account of the World As It Will Be,"pp. 297-298.
[35] Lance J. Hoffman, *Building in Big Brother*, p. 109.

assume then that the Federal Bureau of Investigation (FBI) receives a warrant to implement a wiretap. The wiretap is implemented and the FBI discovers that the communications have been encrypted. The FBI then applies to the key escrow agents for access to the appropriate keys. Presented with a warrant, the key escrow agents release the keys to the FBI. The criminals continue to communicate through what they perceive is a secure medium, but the FBI can now collect the information it needs. Not all encryption systems can implement key escrow and a new system may be required. The benefits of such a system are apparent to law enforcement as it would allow them to access the information they need when they need it. Simultaneously, such a system would allow law-abiding citizens and corporations to communicate securely. It would appear that only the criminals and terrorists have anything to fear from key escrow systems.

During the Clinton administration, a key escrow system known as Clipper was proposed. The goal of Clipper was to implement a key escrow system in hardware. This would allow the system to be physically installed in telephones, modems, and the like. The encryption algorithm chosen is known as SKIPJACK and was developed by the National Security Agency (NSA). SKIPJACK is an 80-bit encryption algorithm whose details were classified. This resulted in significant criticism from the cryptographic community who wished to subject the algorithm to peer review. This policy was in stark contrast to that of the DES, where the information regarding the algorithm was publicly available. The government argued that if details of SKIPJACK were to fall into the hands of possible enemies, it would provide them with strong unbreakable encryption. The government feared that, more likely, a device such as

Deep Crack could be constructed by a third party and be used to decrypt government data if the details became public. To address the concerns of cryptographers, the NSA brought in a small group of encryption experts to evaluate the security of the algorithm. In the limited time they were granted to examine it, they concluded that the algorithm itself was secure from shortcut attacks and that 80-bits was sufficient to prevent brute force efforts.[36]

Unfortunately, there were several other concerns which overshadowed the development of Clipper, mainly involving privacy and economic issues. No one doubted the National Security Agency's ability to construct a secure encryption algorithm, but many doubted the agency's motives. The NSA is shrouded in secrecy:

> The National Security Agency/Central Security Service is America's cryptologic organization. It coordinates, directs and performs highly specialized activities to protect US information systems and produce foreign intelligence information... the NSA employs the country's premier cryptologists. It is said to be the largest employer of mathematicians in the United States and perhaps the world. Its mathematicians contribute directly to the two missions of the Agency: designing cipher systems that will protect the integrity of US information systems and searching for weaknesses in adversaries' systems and codes.[37]

Due to the lack of information available regarding the NSA, most discussions involving it degenerate into conspiracy theories.[38] Many doubted the NSA would be able to resist building a backdoor into Clipper. Whether or not the Agency did is irrelevant because foreign groups refused to consider Clipper or products based upon it for use. Clipper would have been limited then to the American market and domestic corporations were not eager to produce a product under such profit constraints. Even

[36] Brickell, et al., "Skipjack Review," 119-130.

[37] Available from http://www.nsa.gov/about/index.cfm.

[38] John Perry Barlow, "Decrypting the Puzzle Palace," *Communications of the ACM (Association for Computing Machinery)* 35/7 (1992): 25-33.

Americans were not particularly trusting of the NSA and its Clipper chip. The fear of a breach of Fourth and Fifth Amendment rights and protests from various computing industry lobbies eventually resulted in the abandonment of this initiative. The concerns about privacy and Clipper were legitimate. Who could be considered a trusted key escrow holder? Could the state be trusted not to eavesdrop on its citizens when it had the capabilities to do so? Additionally, it became clear to law enforcement that Clipper was not a perfect solution. An individual could encrypt their data twice, first with a non-Clipper product and again with Clipper, a process referred to as super-encryption.[39] This would leave the FBI no better off than before. Ultimately, privacy concerns, the unwillingness of American corporations to produce it and the prospect of super-encryption defeated the key escrow initiative within the United States.[40] Having discussed the failure of the key escrow initiative within the United States, we now turn to export controls.

Export controls are legislation which limits the export of specific items, such as encryption programs, the export of which occurs through a licensing program administrated by the Defense Department and the NSA.[41] Historically, encryption was treated as a military concern but more recently the technology has been reclassified as a dual use one.[42] Export controls had historically limited the strength of encryption that could be exported and also to whom it could be exported. This was largely the result of policy from the Cold War era by which the United States prevented the export of specific

[39] Matt Blaze, "Protocol Failure in the Escrowed Encryption Standard," in *Building in Big Brother*, pp. 131-46.

[40] For a detailed discussion of the privacy issues surrounding Clipper, key escrow and encryption in general, see Lance J. Hoffman, ed., *Building in Big Brother*.

[41] Ibid., pp. 344-345.

[42] James B. Burnham, "The Heavy Hand of Export Controls," *Society* 34/2 (1997): p. 39.

technologies they feared would aid their opponents.[43] The National Security Agency argued for a long time that its intelligence gathering capability would be significantly reduced if strong encryption technology was made widely available to foreign groups. "(Supporters of the NSA's position have) gone so far as to insist that any such items that are exported be modified to ensure that the agency can intercept or decode activity using them."[44] The specific nations affected by this legislation were primarily in the Soviet block and the Third World.[45]

There are two underlying assumptions to the arguments for preventing the export of American encryption products. First, it assumes that American encryption products are stronger than encryption products available from other countries. The algorithm for AES was chosen through an international competition.[46] The selected algorithm was created by two Dutch cryptographers, so clearly there is strong encryption available internationally. Previous discussions have stated that even moderately strong encryption posses a sufficient barrier to information access and that level of encryption is certainly available internationally. Second, it assumes the United States can prevent encryption technology from being distributed internationally. Phil Zimmerman developed the public key encryption system Pretty Good Privacy (PGP), which is regarded as a strong encryption algorithm. After he created it, he gave it away freely on the Internet. The US conducted a lengthy investigation with the intent to prosecute him for violating export control regulations but ultimately laid no charges. [47] By July 2000, it

[43] Ibid., p. 40.

[44] Ibid.

[45] Clark Weissman, "A National Debate on Encryption Exportability," *Communications of the ACM* 34/10 (1991): p. 162.

[46] Black, "Taking Account of the World As It Will Be," p. 295.

[47] Matthew Parker Voors, "Encryption Regulation in the Wake of September 11, 2001: Must We Protect National Security at the Expense of the Economy?" *Federal Communications Law Journal* 55/2 (2003): p. 338 and Philip Zimmerman, "Pretty Good Privacy: Public Key Encryption for the Masses," in *Building in Big Brother*.

was announced that all US companies could freely export encryption products directly to users in a number of selected countries.[48]

The two policy options that the United States attempted to implement failed. From these failures several observations can be made. First, respect for privacy limits the effectiveness of national security policy with regards to encryption. Second, the free flow of information across the Internet, and therefore borders, makes it difficult to restrict the use of encryption products. Third, such products are being created across the world and limiting the export of encryption technology from one nation will not prevent international use of encryption. After September 11th some called for the re-establishment of encryption regulations, but this did not go far, mainly due to past policy failures.[49] Despite the United States' possession of the most resources to deal with this challenge, it appears unable to do so. The information gathering process is sufficiently important to the national security function that encryption's impact upon it is significant. Therefore, the impact of encryption extends to the functional and potential levels of state autonomy.

This paper has examined the information gathering process and the impact that encryption has upon this process, ultimately determining that encryption is capable of impacting potential state autonomy. Encryption was selected as the technology for analysis due to the significance of its interaction with the national security function, the body of policy literature available, and the lack of exploration of this technology by political scientists. It is hoped that this discussion encourages other treatments of technology and the state within the field of political science, as technology is often

[48] Ibid., p. 345.
[49] Ibid., p. 346.

inappropriately considered a secondary factor within that discipline.[50]

[50] The scope of this project prevents full exploration of every topic that has been touched upon. While this paper has focused on the negative impact of encryption upon state autonomy, there is the potential for positive benefits from this technology as well. Future research will explore whether the potential positive benefits are sufficient to offset the negative impact. Privacy concerns were only briefly discussed in this paper, but there is a significant body of literature exploring the interaction between the state and privacy, and recently, encryption and privacy. The body of literature surrounding cryptography policy, its development, its failure, and the unique lobbying efforts surrounding its failure will be further explored. Along with the hierarchy of state autonomy, the framework of analysis created for this project will be employed in other projects and has been expanded upon in other work that explores what constitutes voluntary and involuntary state action in the international system.