California Legal Studies Journal

University of California, Berkeley
Fall 2009-Spring 2010

Table of Contents

The New Code War:
A Discourse in the Legal Framework for State-To-State Cyber Attacks and Cyber Warfare

By Michael Iseri

I. Introduction: "What are the rights of a country victimized by cyber attacks?"

"We know that if someone shoots missiles at us, they're going to get a certain kind of response. What happens if it comes over the Internet?" - Michael Chertoff, former Homeland Security Secretary[1]

On November 11, 2008, China unlawfully breached the White House's mail systems.[2] On November of 2008, Russian hackers were suspected of penetrating the Pentagon's security systems and gaining access to sensitive information.[3] Yet, the responses to these attacks were bizarre. While the attacks were detected by United States' security agencies, the public outcry was minimal and the physical repercussions nonexistent. The reason: these attacks were not physical attacks or intrusions; rather they were cyber attacks, a growing threat to nation–states. For the White House's mail incident, China hacked and gained access to the White House's e-mail servers through both network penetration and an information collecting technique called "grain of sands," a technique that collects large amounts of data to find scattered vital information.[4] For the Pentagon's networks, a malware program known as "agent.btz" spread through USB flash drives and infected the US Central Command systems: the headquarter for U.S.

---

[1] Randall Mikkelsen, "U.S. not ready for cyber attack," Reuters, 19 Dec. 2008, Web, 22 Mar. 2010 <http://www.reuters.com/article/domesticNews/idUSTRE4BI00520081219>.

[2] Kevin Coleman, "China Hacks White House Email?" DefenseTech, Ed. Christian Lowe, 11 Nov. 2008, Military.com, Web, 22 Mar. 2010 <http://www.defensetech.org/archives/004524.html>.

[3] Julian E. Barnes, "Pentagon Computer Networks Attacked," Los Angeles Times 28 Nov. 2008: 1-3, Web, 10 Jan. 2010. <http://articles.latimes.com/2008/nov/28/nation/na-cyberattack28>.

[4] Coleman, "China Hacks White House Email?."

involvement in Iraq and Afghanistan.[5] It is believed that this program originated from within Russia.[6]

These cyber attacks are just two out of 2.5 million and growing cyber attacks occurring each day around the world, and they will continue to grow as more computer networks become interwoven into vital parts of societies and governments.[7] Based on past precedents, a country that is the victim of state-sponsored cyber attacks has limited rights concerning self-defense or retaliation. Furthermore, current laws are inadequate in preventing or stopping these cyber attacks. These problems have created a void in the international legal framework concerning the treatment of cyber attacks. This void has paralyzed governments and alliances in responding promptly and properly to state-sponsored cyber attacks, limiting a victimized country's capacity to respond to state-sponsored cyber attacks or cyber warfare. Michal Chertoff, former Homeland Security Secretary, predicted that cyber attacks will be a viable method for future warfare by giving the attacker an opportunity to degrade a country's command infrastructure before a physical attack.[8] He further warns that international laws and military doctrines need to be changed to accommodate this new growing threat.[9] Government sanctioned cyber attacks have occurred in the past: Moonlight Maze,[10] Titan Rain, and the 2001 spy plane

---

[5] Barnes 1-3.
[6] Ibid.
[7] David Neal, "Security attacks reach 2.5 billion per day." Vnunet, 5 Dec. 2008, Web, 22 Mar. 2010 <http://www.vnunet.com/vnunet/news/2232104/ibm-boosts-security-services>.
[8] Mikkelsen, "U.S. not ready for cyber attack."
[9] Ibid.
[10] "The Warnings?" Cyber War! 24 Apr. 2003. Frontline,PBS. Web. 22 Mar. 2010 <http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/warnings/>.

incident between China and the United States.[11] Recent cyber attacks are even more destructive and more intrusive: the Estonian cyber attacks of 2007, the Russia-Georgia conflict, and GhostNet. Cyber attacks are now part of a country's arsenal for modern warfare, and international legal frameworks need to change to accommodate and handle these growing threats.

This paper will discuss three major cyber attacks: the Estonian cyber attacks of 2007, the Russian-Georgia conflict, and GhostNet. The Estonian cyber attacks of 2007 showed the inadequacies in NATO's legal framework to define the rights for a victimized country of state-sponsored cyber attacks. The Russia-Georgia conflict highlighted the problems with United Nation's legal framework when responding to state-sponsored cyber attacks and the issues with identifying the main attacker for cyber attacks. Lastly, GhostNet tested the gray boundaries of acceptability concerning cyber attacks, questioning where the legal line should be drawn for legal frameworks to govern cyber attacks.

The aim of this paper is twofold. First, to describe the complexities of cyber attacks by exploring the components of cyber attacks and how they occur; and second, to examine how cyber attacks are being handled by governments and their international legal frameworks. It is with the best intentions that this paper will contribute to the examination and further discussions of the developing international legal frameworks concerning state-sponsored cyber attacks and cyber warfare.

---

[11] Kevin Poulsen, "Threat Level Privacy, Crime and Security Online 'Cyberwar' and Estonia's Panic
Attack," Threat Level, 22 July 2007, Wired, Web, 22 Mar. 2010
<http://www.wired.com/threatlevel/
2007/08/ cyber-war-and-e/>.

II. Defining Cyber Attacks and Cyber Warfare

"Cyber defence remains, in many ways, an immature discipline... [National security experts warn:] *'Expect disruptive cyber activities to be the norm in future political or military conflicts.'"* - NATO 2009 Spring Session[12]

A new battleground has emerged. Instead of using missiles that destroy infrastructures and kill people, an attacker can utilize numerous computer vulnerabilities that penetrate, interfere, disrupt, disable, steal, or destroy communications, vital information, and operating systems on numerous computer systems and networks. These attacks are known as cyber attacks, with the vast majority of cyber attacks utilizing "vulnerabilities in networks, operating systems, and applications" to accomplish the attacker's goals.[13] In the past, cyber attacks were handled by extending traditional laws and policies concerning physical warfare through analogies. However, current international laws and policies are inadequate for handling cyber attacks for one main reason: there is a void in international legal frameworks for detailing a country's rights to respond as a victim to a state sponsored cyber attacks. Should a country respond to state-sponsored cyber attacks with physical force? As of this writing, there exists no transparent or uniform answer amongst alliances that handle cyber attacks and cyber warfare.

State-sponsored cyber attacks have created a new type of warfare: cyber warfare. Cyber warfare has no static definition. According to NATO's 2009 Spring Session, there is "no

---

[12] North Atlantic Treaty Organization, NATO Parliamentary Assembly, "027 DSCFC 09 E - NATO and Cyber Defence," 2009 Spring Session, Sverre Myrli, Section 17, NATO Committee Reports, 10 May 2009 <http://natopa.ibicenter.net/default.asp?SHORTCUT=1782>.

[13] Greg White, et al. CompTIA Security+ All-In-One Exam Guide, Second Edition, 2nd ed. N.p., McGraw-Hill Companies, 2009. 416.

international legal consensus exists on what the terms 'cyber war,'[or] 'cyber attack'" mean.[14] There are two major schools of thought concerning what constitutes cyber warfare. One group believes that cyber warfare must be a series of cyber attacks that coincide with an actual physical attack.[15] Others believe that cyber warfare must be a "digital Pearl Harbor" attack, an attack that is a purely Internet based.[16] As of this writing, there have been two major cyber attack incidents that could be classified in one of these two categories: the Estonian cyber attacks of 2007 and the Russia-Georgia conflict. The Estonian cyber attacks of 2007 is considered a pure "digital Pearl Harbor" attack while the Russia-Georgia conflict is physical warfare that incorporated cyber attacks strategically.

There are two problems that make cyber attacks difficult for any legal framework to govern them: one is identifying the attackers, and the other is determining the intentions of the attacks. For the first problem, cyber attacks can originate from governments, government-affiliated hacker groups, individuals, or a combination of all the above. For the victim to respond properly to a cyber attack, that victim must identify the attackers. By knowing the attackers, the victim can determine an appropriate response that is suitable for that situation. This paper will examine cyber attacks that originate either from a state-government or a government-affiliated hacker group. This is not to disregard the severity of individual based cyber attacks, but the topic of rogue individuals and their motives to commit cyber attacks is too vast for this topic. The second problem is determining the intentions of an attacker for committing cyber attacks. By knowing the intentions of an attacker, the victim can

---

[14] North Atlantic Treaty Organization, "027 DSCFC 09 E - NATO and Cyber Defence," Section 21.

[15] "Marching Off To Cyberwar." The Economist 4 Dec. 2008. Technology Quarterly. Web. 22 Mar. 2010 <http://www.economist.com/science/tq/displaystory.cfm?story_id=12673385>.

[16] Ibid.

determine the promptness and severity of a response. Solving these two problems would greatly affect how state-sponsored cyber attacks and cyber warfare are investigated and prosecuted.

Cyber attacks are capable of striking global computer networks across the world with ease. Before the advent of cyber attacks, physical attacks or physical reconnaissance were needed in order to breach computer networks and facilities. But due to the creation and the evolution of the Internet, these attacks can now be done through cyberspace. Cyberspace has allowed for attacks and reconnaissance to be done quickly, efficiently, and almost anonymously over the Internet.[17] Furthermore, the Internet has become so ingrained with everyday operations for "power, transportation, communications, banking and finance, and defense" that today's cyber attacks are more destructive and occur more frequently than cyber attacks of years ago.[18] Today, cyber attacks are capable of causing immense economic damages or even loss of human life, such as temporally shutting down the power grid for banks and hospitals.[19]

As the Internet becomes more integrated with everyday operations, cyber attacks become easier to perform and are capable of hitting more critical targets. The reason why cyber attacks are easy to conduct is based on the original purpose of the Internet. The Internet originally was designed to share information, not to provide secure transmissions. The Internet is a mesh network, where every node contains numerous connections to other nodes,[20] that are

---

[17] Howard F. Lipson, Ph.D., Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues, Ed. Pamela Curtis and Mindi McDowell, Springfield: U.S. Department of Commerce, 2002. 3. Nov. 2002, : 3, CERT® Coordination Center, Web, 22 Mar. 2010 <www.cert.org/archive/pdf/02sr009.pdf>.

[18] Ibid.

[19] Ibid. 11.

[20] "Mesh Network," SearchNetworking, 3 Nov. 2006, Web, 22 Mar. 2010 <http://searchnetworking.techtarget.com/

capable of functioning even after portions of the network are destroyed, such as in an event of nuclear war.[21] The chief purpose of the Internet was to provide numerous paths for transmitting information. Security for the Internet was an afterthought.

The greatest strength of the Internet also contributes to its greatest vulnerability: the ability to access information on a single computer terminal by navigating through multiple routes. Howard F. Lipson lists twelve problems with the Internet that makes identifying and locating cyber attacks problematic in his article *Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues*.[22] Lipson names the twelve "shortfall[s] in the current Internet environment" as:

1) The Internet was never designed for tracking and tracing user behavior;
2) The Internet was not designed to resist highly untrustworthy users;
3) A packet's source address is untrustworthy, which severely hinders tracking;
4) The current threat environment far exceeds the Internet's design parameters;
5) The expertise of the average system administrator continues to decline;
6) Attacks often cross multiple administrative, jurisdictional, and national boundaries;
7) Hi-Speed traffic hinders tracking;
8) Tunnels impede tracking;
9) Hackers destroy logs and other audit data;
10) Anonymizers protect privacy by impeding tracking;

---

sDefinition/0,,sid7_gci870763,00.html>.

[21] Walt Howe, "A Brief History of the Internet," Walt Howe's Internet Learning Center, 1 Sept. 2009, Web, 22 Mar. 2010 <http://www.walthowe.com/navnet/history.html>.

[22] Lipson 3.

11) The ability to link specific users to specific IP addresses is being lost;
12) Purely defensive approaches will fail, so deterrence through tracking and tracing is crucial;[23]

To summarize the twelve points, the Internet is not secure. The simplicity of the Internet (problems 1-4), the wide spread proliferation of the Internet (problems 5-7), and the development of tools and methods that overcome the shortfalls with the Internet (problems 8-12) all contribute to the Internet's weak security. Cyber attacks are problematic based on all of the twelve reasons, but two of these twelve problems allow cyber attacks to flourish in everyday operations: problem five, "The expertise of the average system administrator continues to decline," and problem twelve, "Purely defensive approaches will fail, so deterrence through tracking and tracing is crucial." Problem five highlights the real problem for state-sponsored cyber attacks, attackers do not need to target government facilities to cause damage. Attackers can target the financial institutes or power grids, testing the skills of system administrators at those institutes rather than the skills of system administrators in governments. Problem twelve highlights the forgotten truth for all computer networks: there is no perfect defense. There will always be ways for attackers to succeed, and having a purely defensive stance will not ensure full protection of a computer system. Problem twelve also stresses the continual need for governments to research and to develop better cyber security and tracing programs.

III. Cyber Attacks: How Ones and Zeroes Can Cripple Governments

First and foremost, physical security is the highest priority for all security measures, including cyber security.[24] Without physical security, the machines and networks that are being

[23] Ibid. 13-21.
[24] White 185.

protected by cyber security can be stolen or destroyed. There is no reason for developing an elaborate cyber network that protects vital digital information when the actual physical security is porous and easily broken into, "no matter how impenetrable the firewall and intrusion detection system (IDS), if an attacker can find a way to walk up to and touch a server, he can break it."[25] Physical security prevents an attacker from physically tampering, destroying, or stealing computers, servers, or equipment. It is easier for an attacker to retrieve information on a hard drive when that object is in his own possession rather than attempting to steal that same information over the Internet. For governments, physical security is one of the governments' greatest assets as it is crucial to a government's survival. However, the stronger the physical security is for a government, the more appealing cyber attacks become for an attacking government.

There are four steps that most attackers follow before conducting cyber attacks: reconnaissance, scanning, researching vulnerabilities, and performing the attack.[26] The first step, reconnaissance, involves profiling the target by gathering as much information as possible from the target. The information that is useful for cyber attacks are "IP addresses, phone numbers, names of important individuals, and what networks the organization maintains."[27] For governments, information regarding networks and systems would be either very secretive or very public. For example, *The Washington Post* published an article that when Obama's administration moved into the White House, they complained about the White House's computer systems. The administration publically stated that the White House computers were running six-year-old Microsoft software, which would have been Microsoft XP operating

[25] Ibid.
[26] Ibid. 392.
[27] Ibid.

system and Microsoft Office 2003.[28] If knowledge is power, then any information concerning a government's systems is important for cyber attacks. Governments will continually seek out any information concerning other governments' computer systems. Hopefully, the White House has changed their operating systems and programs or significantly improved cyber security of their systems after making their systems publically known.

The second step, scanning, involves creating a list of all the services that are running on active and reachable computers.[29] This step often involves ping sweeps, a method that sends pings to a particular IP address to verify that address and to check if the computer with that IP address is accessible, and port scanning, a method that guesses the computer services running on a system by observing the open ports of a machine.[30] Government networks are not immune to scanning, especially since they are usually the most sought out targets in cyberspace. Scanning is an extremely powerful technique as it provides attackers with vital information concerning the computers' operating systems and applications that are running within a target network.[31] Governmental systems will always be targets of scans, whether from other governments or from individuals.

The next step involves researching the vulnerabilities of networks, operating systems, applications or services, and users of an institute.[32] For this step, the attacker has one of the most powerful tools aiding him in his research: the Internet. There are numerous

---

[28] Anne E. Komblut, "Staff Finds White House in the Technological Dark Ages," *The Washington Post*, N.p., 22 Jan. 2009, Web, 22 Mar. 2010 <http://www.washingtonpost.com/wp-dyn/content/article/2009/01/21/AR2009012104249.html>.

[29] White 392-393.

[30] Ibid. 392.

[31] Ibid. 393.

[32] Ibid.

websites and forums that detail recently discovered or known vulnerabilities for software, protocols, and operating systems.[33] These websites exist to aid computer administrators with their systems and networks, but the same information can be used to aid attackers, allowing attackers to develop malicious programs or techniques within a short time span.[34] For example, Microsoft released a security patch on October 2008.[35] Information concerning the vulnerabilities that the patch fixed was discovered a month later. A virus known as "Conficker.A" was released online on November 21, 2008, and it sought out and infected computers that did not install the October 2008 security patch.[36] The Conficker virus "died" on April 2009 after an extensive push to eliminate the virus, ending its life on the fifth iteration of the virus, "Conficker.E."[37] In addition, various administrator tools and programs can be found on numerous websites that aid administrators in their network security, but the same tools can be applied and used for cyber attacks.[38]

The last step is performing the cyber attack.[39] As stated before, there exists no perfect defense for computer systems. Take the following as an analogy of how breaking into a house is similar to breaking into a computer. There is a house, and a thief who wants to get inside that house. A lock on the house's door may be enough to deter the thief from attempting to break into that house. However, if a thief is motivated to break into that particular house, he can try numerous methods to get inside that house. For example, the thief

---

[33] Ibid.
[34] Ibid.
[35] "Conficker: FAQ," Conficker Working Group, 26 Mar. 2009, Web, 22 Mar. 2010 <http://www.confickerworkinggroup.org/wiki/pmwiki.php/ANY/FAQ>.
[36] "Conficker: Timeline," Conficker Working Group, 26 Apr. 2009, Web, 22 Mar. 2010 <http://www.confickerworkinggroup.org/wiki/pmwiki.php/ANY/Timeline>.
[37] Ibid.
[38] White 393.
[39] Ibid.

could try picking the lock, going through the backdoor or windows, tricking the owner into letting him in, ambushing the person who opened the door, employing other thieves to aid him, using a forge key, or breaking down the front door. Once in, the thief can accomplish whatever he wants. Similarly, an attacker has numerous methods to break into a computer system to shut down networks, deface websites, alter information, and much more.[40] Cyber attacks are only limited to an attacker's imagination.[41]

IV. Methods for Cyber Attacks:

The following is a list of well known methods that can be used for committing cyber attacks: denial-of-service attacks (DoS), distributed denial-of-service attacks (DDoS), botnets, rootkits, and social engineering.[42] Other methods for cyber attacks that will not be discussed in this paper are backdoors, sniffing, spoofing, man-in-the-middle attacks, attacks on encryption, password guessing, software exploitation, malicious codes, Trojan horses, spyware, logic bombs, worms, and application level attacks. This list is by no means complete as there exist other methods for cyber attacks, including undiscovered means of attacks.

IV.a. Denial-of-Service Attacks (DoS) and Distributed Denial-of-Service Attacks (DDoS):

Denial-of-service (DoS) attacks and distributed denial-of-service (DDoS) attacks prevent the user from accessing specific information on a system or a network by disabling the system or the network.[43] To succeed, a DoS attack or a DDoS attack needs to crash or to overload the system with requests, allowing the attacker the

[40] Ibid. 393-394.
[41] Ibid. 393.
[42] Ibid. 394-417.
[43] Ibid. 395.

opportunity to commit further actions unnoticed.[44] A DoS attack uses only one system to commit the attack while a DDoS attack uses multiple attacking systems, often employing large armies of computers known as botnets. Out of the two, DDoS attacks are the more difficult to prevent.

A DDoS attack denies services to users by overwhelming the target's network with traffic from different systems. A DDoS attack is a DoS attack that uses an army of hundreds or thousands of machines to launch a many-against-one-attack.[45] Often, an attacker uses botnets, a large network of unwilling, infected machines that are controlled by malicious programs. The benefit of using a botnet is that an attacker can hide his identity by having other machines committing the cyber attacks. Governments do not need botnets to use DDoS attacks, but they can use them if they want to mask their identity. Instead, governments have vast resources available that allow them to acquire thousands of computers, making DDoS attacks a viable option for them to perform.

Little can be done to prevent a massive, coordinated DDoS attack on a specific target. If a DDoS attack is large enough, "any network, no matter how much the load is distributed, can be successfully attacked."[46] To prevent a DDoS attack, either the DDoS attack messages or the connections from a DDoS network must be intercepted or blocked by the targeted system, which is difficult to do.[47] For these reasons, DDoS attacks are well suited for state-sponsored cyber attacks.

---

[44] Ibid. 394-395.
[45] Ibid. 587.
[46] Ibid. 397.
[47] Ibid.

IV.b. Botnets:

"A botnet is comparable to compulsory military service for windows boxes" - Stromberg[48]

A botnet is a group of controlled computers over which an attacker has complete control.[49] Usually, an attacker establishes a botnet by infecting numerous machines with programs that grant him control over the systems, often without the owners' knowledge. Botnets provide the attacker with nearly endless computer processing and bandwidth connections, as a single botnet can control an army of thousands to hundreds of thousands of computers that are fully capable of conducting synchronized cyber attacks.[50] Botnets are deadly tools for cyber attacks, especially since they are one of the best tools for committing DDoS attacks anonymously.

IV.c. Rootkits:

A rootkit modifies an operating system to facilitate nonstandard functionality.[51] Rootkits allow an attacker to do anything that an operating system does, including keylogging, sniffing, hiding files and applications, creating backdoors, and processing files on a system without alerting either the user or other programs.[52]

IV.d. Social Engineering:

---

[48] Drupal, "Use Of Botnets," The Honeynet Project, 10 Aug. 2008, Web, 22 Mar. 2010 <http://www.honeynet.org/ node/52>.

[49] "Bots and Botnets— A Growing Threat," Norton From Symantec, Web, 22 Mar. 2010 <http://www.symantec.com/ norton/theme.jsp?themeid=botnet>.

[50] "Botnet," SearchSecurity, 30 Oct. 2008, Web, 22 Mar. 2010 <http://searchsecurity.techtarget.com/sDefinition/ 0,,sid14_gci1030284,00.html>.

[51] Ibid. 413.

[52] Ibid. 414.

Social engineering involves the attacker using social methods to misrepresent and to deceive users in order to gain access to a target network.[53] The attacker can pretend to be a pizza delivery person to gain access to a building, make phone calls to the administrators requesting a password reset to an authorized user account that the attacker has access to, use phishing e-mails to obtain valuable information such as user names and passwords, and much more. "Phishing" involves the attacker attempting to obtain information through e-mails by impersonating a trusted source. Phishing schemes that target specific institutions, such as corporations or governments, are known as "whaling" and "spear phishing".[54] Instead of casting out a wide net that is common for "phishing" scams, "whaling" and "spear phishing" target a "big phish," such as high-ranking officials or executives.[55] Social engineering succeeds by targeting the weakest part of cyber security, the users.

V. The Significance of an International Legal Framework for Cyber Attacks

"…No binding international law on cyber security exists which expresses the common will of countries and which can serve as a basis for shaping national laws. As this is a rapidly developing field

---

[53] Ibid. 416.

[54] "Spear Phishing and Whaling Attacks Reach Record Levels," iDefense Labs, 7 June 2008, Web, 22 Mar. 2010 <http://labs.idefense.com/news/press/bbb/>.

[55] AFP, "Hackers harpoon executives in 'whaling' attacks," The Sydney Morning Herald, 6 May 2008, Web, 10 May 2009 <http://www.smh.com.au/news/security/hackers-harpoon-executives-in-whaling-attacks/2008/05/06/1209839606696.html>.

of law, all possible cyber threats have yet to be defined" - Ministry of Defense, Estonia[56]

The report *Cyber Security Strategy*, issued by Estonia's Ministry of Defense, details the goals for the development of international legal frameworks for cyber attacks while examining the numerous deficiencies found within current international legal frameworks for cyber attacks. There are two types of cyber attack that an international legal frameworks needs to address: 1. when the cyber attack occurs within a country, and 2. when a cyber attack involves numerous countries.[57] Most countries have pre-existing cyber laws that handle cyber attacks that are confined within their boundaries. However, cyber attacks that involve multiple countries require an international legal framework that promotes international legal instruments and bilateral agreements.[58] Most importantly, an international legal framework needs to establish these instruments and agreements for cyber attacks on a global level.[59] The main goals for establishing an international legal framework are as follows:

- Development of legal definitions for cyber security and cyber crime;
- Development and implementation of legislation to ensure cyber security, including the introduction of compulsory security measures and standards in critical infrastructure companies and the establishment of minimum

---

[56] Estonia, Cyber Security Strategy Committee, "3.4.1. International Law," *Cyber Security Strategy*, 17,
Estonian Ministry of Defence, N.p., 2008, Web, 23 Mar. 2010 <http://www.mod.gov.ee/files/kmin/img/files/Kuberjulgeoleku_strateegia_2008-2013_ENG.pdf>.[PDF file accessed from English version of Estonian Ministry of Defence, National Defense and Society: Cyber Security <http://www.mod.gov.ee/en/national-defense-and-society> (Last updated 23 Mar. 2010)]

[57] Ibid.

[58] Ibid.

[59] Ibid. "3.5. International Co-Operation," 21.

information security requirements for all information systems;
- Improvement of existing legislation with a view to ensuring cyber security;
- Drafting of new legislation to cover new areas or threats;
- Launching of initiatives in international law-making.[60]

An international legal framework would allow for wide-spread proliferation and acceptance of global cyber terminology, protocols, and procedures for cyber attacks. Furthermore, the international legal framework needs to incorporate revised pre-existing laws such as penal codes, an electronic communications act (which establishes general requirements of an information infrastructure), a personal data protection act (which establishes the levels of security that a state needs to provide to collected information for processing), a public information act (which establishes how a government accesses public information), and an information society services act (which limits the liability for ISPs concerning investigations).[61] Only through co-operative efforts can governments and alliances develop international legal frameworks that strengthen the global cyber culture.[62]

There are two established international legal frameworks that govern cyber threats but are problematic when handling state-sponsored cyber attacks: the Council of Europe Convention on Cybercrime and the European Union's legal framework.[63] The main problem with both legal frameworks is how they label cyber attacks that target "critical infrastructure information systems" as attacks against ordinary computer infrastructures rather than serious threats. By labeling these cyber attacks as attacks against ordinary computer infrastructures, both frameworks can only treat these cyber attacks as

[60] Ibid. "4.3 Development of a Legal Framework for Cyber Security," 30-31.
[61] Ibid. "3.4.2. National Legal Framework," 18-21.
[62] Ibid. "3.5. International Co-Operation," 21.
[63] Ibid. "3.4.1. International Law," 17.

criminal offences and not as critical governmental security threats.[64] Another problem is the low number of participating countries. As of the beginning of 2010, only 26 out of the 60 countries from the Council of Europe have amended their legislatures to incorporate the Convention on Cybercrime.[65] Similarly, the EU legal framework's power of influence is limited only to its members and not to non-EU countries.[66]

These legal frameworks are inadequate for addressing the new growing threat of cyber attacks. Nevertheless, there are two more developing international legal frameworks that show promise for addressing the shortfalls found within the Council of Europe and the EU's legal frameworks: NATO and the UN. The remainder of this paper will explore NATO and the UN's developing international legal frameworks for cyber attacks by examining how each alliance responds to current state-sponsored cyber attacks.

VI. The Estonia Cyber Attack of 2007

"[Estonia,] NATO's most IT-savvy nation" - Jaap de Hoop Scheffer, NATO Secretary-General [67]

On April 27, 2007, Estonia relocated the Bronze Soldier Soviet war memorial from Tallinn and started excavating World War II Red Army graves.[68] Although the Bronze Soldier memorial is

---

[64] Ibid. "3.4.1. International Law," 18.

[65] "Convention on Cybercrime CETS No.: 185," *Council of Europe*, N.p., 4 Jan. 2010, Web, 9 Jan. 2010 <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=04/01/2010&CL=ENG>.

[66] Cyber Security Strategy Committee. "3.4.1. International Law," 18.

[67] Ahto Lobjakas, "News Analysis: How Vulnerable Are Countries To Cyberattacks? Ask Estonia!," Radio Free Europe/Radio Liberty, 29 Apr. 2008, Web, 22 Mar. 2010 <http://www.rferl.org/content/Article/1109653.html>.

[68] John Leyden, "Estonian/Russian statue riots spill online," The Register, 1 May 2007, Web, 22 Mar. 2010 <http://www.theregister.co.uk/2007/05/01/estonian_riots/>.

dedicated to the Soviet soldiers who fought against the Nazis during World War II, many Estonians perceived the statue as a symbol of five decades of Soviet occupation.[69] For three days after the Bronze Soldier removal, pro-ethnic Russian rioters clashed with Estonia's police in numerous protests, resulting in 150 injuries and a man being stabbed to death.[70] During the same time, another conflict erupted between Estonia and Russia: a battle in the borderless cyber space. For the next three weeks, a series of coordinated DDoS cyber attacks targeted Estonia's Internet infrastructure, crippling its communications and online transactions.[71] This marked the first time that a "broad and sustained attack from the Internet" had targeted a single country.[72]

These cyber attacks, which were believed to have originated in Russia, devastated Estonia's economy. Estonia is the pinnacle of e-government with paperless government meetings, Internet voting, online taxpaying, e-schools, and even the ability to pay for parking via text message.[73] Yet, Estonia's economy came to a sudden halt when coordinated cyber attacks, peaking at one million remotely controlled computers, severely disrupted and disabled Estonia's Internet infrastructure.[74] At the peak of these cyber attacks, Estonia lost 50% of its bread, milk, and gasoline sales for 90 minutes, and another 75% of these commodities for 5 minutes.[75] The severest

---

[69] AFP, "Hacker Convicted In 'Cyber-War,'" FRANCE 24, 23 Jan. 2008, 22 Mar. 2010 <http://www.france24.com/en/20080123-hacker-convicted-cyber-war-estonia-justice>.
[70] Leyden, "Estonian/Russian statue riots spill online."
[71] Ian Traynor, "Russia Accused of Unleashing Cyberwar to Disable Estonia," Guardian News and Media Limited, 17 May 2007, Web, 22 Mar. 2010 <http://www.guardian.co.uk/world/2007/may/17/topstories3.russia>.
[72] Lobjakas, "News Analysis: How Vulnerable Are Countries To Cyberattacks? Ask Estonia!."
[73] Ibid.
[74] Ibid.
[75] Ibid.

damage occurred in May when the networks for Estonia's biggest bank, Hansapank, stuttered due the high volume of cyber attacks, causing sporadic disruptions of business and credit card transactions.[76] There were three notable peaks of cyber attacks during the three-week period: May 3, five days after the Bronze Soldier was removed, May 8-9, Russia's Victory Day over Germany and the day when Vladimir Putin delivered a hostile speech attacking Estonia and indirectly linked the Bush administration to the Hitler regime, and again in Mid-May of 2007.[77] The cyber attacks affected the networks of the "Estonian presidency and its parliament, almost all of the country's government ministries, political parties, three of the country's six big news organizations, and two of the biggest banks."[78] All of this happened without a single physical attack.

VII. NATO's Response, the Development of the Current International Legal Framework for Cyber Attacks and Cyber Warfare

What can a country do if it is a victim of cyber attacks? The Estonian cyber attacks of 2007 showed how current international laws and policies were inadequate in addressing and reacting to cyber attacks. These cyber attacks devastated Estonia's economy, and Estonia's Defense Minister Jaak Aaviksoo analogizes these attacks to that of a blockade of sea ports, in which "a nation's access to the world could be denied."[79] Estonia, a NATO member since 2004, requested NATO to help diffuse the problem.

The main problem with the Estonian cyber attacks was identifying the attacker. Estonia traced the cyber attacks and

---

[76] Ibid.
[77] Traynor, "Russia accused of unleashing cyberwar to disable Estonia."
[78] Ibid.
[79] North Atlantic Treaty Organization, "027 DSCFC 09 E - NATO and Cyber Defence," Section 52.

concluded that the attacks were originating from Russia.[80] Estonia informed NATO of these cyber attacks and accused Russia's government as being the main instigator.[81] However, there were problems in conclusively identifying Russia as the main instigator of these cyber attacks. A beneficial trait of cyber attacks is that the attacker can remain anonymous, allowing him the ability to deny conducting these attacks. The earliest wave of cyber attacks were traced back to Russia's governmental computers, but the majority of later cyber attacks came from the computers of pro-Russia users.[82] Due to both the anonymous nature of cyber attacks and the wide range of actors who were involved with these cyber attacks, Estonia could not conclusively link Russia's government as the main orchestrator for these cyber attacks. Furthermore, the Kremlin denied any involvements with these cyber attacks. Dmitry Peskov, the Kremlin's chief spokesman stated there was "no way the [Russian] state [could] be involved in cyber terrorism."[83] Furthermore, Russia refused to provide aid or to cooperate with Estonia in shutting down the computers that were conducting these cyber attacks.[84]

Estonia had one of two options: one, take a defensive stance and try to prevent further cyber attacks from disabling and harming their networked infrastructures; or two, take an offensive stance and invoke NATO's article 5, the "collective self-defense" clause. NATO's Article V states:

---

[80] "The Cyber Raiders Hitting Estonia," BBC News, 17 May 2007, 22 Mar. 2010 <http://news.bbc.co.uk/2/hi/ europe/6665195.stm>.

[81] United States, Cong. The NATO Summit at Bucharest, 2008, By Paul Gallis, The Library of Congress, 2008, CRS Report for Congress, 5 May 2008, Congressional Research Service,Web, 22 Mar. 2010 <http://www.fas.org/sgp/crs/row/RS22847.pdf>.

[82] Traynor, "Russia accused of unleashing cyberwar to disable Estonia.".

[83] "The Cyber Raiders Hitting Estonia," BBC News.

[84] North Atlantic Treaty Organization, "027 DSCFC 09 E - NATO and Cyber Defence," Section 24.

> The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defence recognised by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area.[85]

If cyber attacks are classified as an "armed attack," then state-sponsored cyber attacks against one NATO ally is an attack on all NATO allies, permitting the use of armed forces "to restore and maintain the security of North Atlantic area."[86] The only time Article 5 has been invoked was following the September 11, 2001 attacks on the United States.[87] Estonia's defense minister Jaak Aaviksoo considered invoking Article 5 as a response to the cyber attacks; however there were two problems in using Article 5.[88] The first problem: there must be a general consensus among NATO's alliance members agreeing that cyber attacks constitute an "armed attack." Cyber attacks can cause as much damage, if not more, than physical armed attacks, yet there is not a unanimous agreement that cyber attacks are "armed attacks," let alone an actual definition of what constitutes a cyber attack. The second problem: Estonia needed the support of NATO's alliance members for any action to be taken as a

---

[85] North Atlantic Treaty Organization, "Article 5," The North Atlantic Treaty: 4 April 1949, Washington D.C., 1949, On-Line Library, 29 Nov. 2007, Web, 22 Mar. 2010 <http://www.nato.int/docu/basictxt/treaty.htm>.

[86] Poulsen, "Threat Level Privacy, Crime and Security Online 'Cyberwar' and Estonia's Panic Attack."

[87] North Atlantic Treaty Organization, "027 DSCFC 09 E - NATO and Cyber Defence," Section 51.

[88] Poulsen, "Threat Level Privacy, Crime and Security Online 'Cyberwar' and Estonia's Panic Attack."

response to these cyber attacks. The alliance members would have had to support Estonia's right to protect itself against further attacks. NATO did not want its members to be at war with Russia. Ultimately, NATO did not support Estonia's proposal to retaliate to these cyber attacks since there existed no conclusive evidence that linked Russia's government to these cyber attacks.

A year after the Estonian cyber attacks, NATO made clear its stance on cyber attacks at the April 2008 summit in Bucharest.[89] During the summit, NATO decided that "the allies are not at the point where [a cyber attack]… would be considered an Article V crisis, leading to a call for mutual defense."[90] Furthermore, under Article 47 of the 2008 Bucharest Summit Declaration, NATO will treat cyber attacks as follows:

> NATO remains committed to strengthening key Alliance information systems against cyber attacks. We have recently adopted a Policy on Cyber Defence, and are developing the structures and authorities to carry it out. Our Policy on Cyber Defence emphasises the need for NATO and nations to protect key information systems in accordance with their respective responsibilities; share best practices; and provide a capability to assist Allied nations, upon request, to counter a cyber attack. We look forward to continuing the development of NATO's cyber defence capabilities and strengthening the linkages between NATO and national authorities.[91]

NATO will provide assistance to NATO members who are targets of cyber attacks, but each member is responsible for protecting their own critical networked infrastructures. NATO is seeking to find an

---

[89] Lobjakas, "News Analysis: How Vulnerable Are Countries To Cyberattacks? Ask Estonia!."

[90] The NATO Summit at Bucharest, 2008, 2-3.

[91] North Atlantic Treaty Organization, "Article 47," Bucharest Summit Declaration: 3 April 2008, Bucharest, 2008, 16 Mar. 2009, Web, 22 Mar. 2010 <http://www.nato.int/cps/en/natolive/official_texts_8443.htm >.

appropriate response to cyber attacks, but it has yet to come to an agreed upon solution amongst its members.

Today, Estonia is at the forefront in establishing laws and preventive measurements for handling cyber attacks amongst NATO alliance members. On May 14, 2008, NATO established the Cooperative Cyber Defense Center of Excellence (CCD CoE) in Estonia as a response to Article 47 of the Bucharest Summit Declaration of 2008.[92] Previously, Estonia tried to develop this center back in 2003, but the Estonian cyber attacks of 2007 sparked a renewed interest amongst NATO members.[93] As of November 11, 2008, eight nations have joined the CCD COE: Estonia, Germany, Italy, Latvia, Lithuania, Spain, the Slovak Republic, and the United States.[94] On October 28, 2008, the North-Atlantic Council granted CCD CoE full accreditation and International Military Organization status.[95] The main tasks of the CCD CoE include:

1) Providing cyber-related doctrines and concepts for the Alliance;
2) Hosting and conducting training workshops, courses, and exercises for NATO member states;
3) Conducting research and development activities;
4) Studying past or ongoing attacks to draw up lessons learned;

---

[92] "NATO Opens New Centre of Excellence on Cyber Defence," NATO, 20 May 2008, North Atlantic Treaty Organization, Web, 22 Mar. 2010 <http://www.nato.int/docu/update/2008/05-may/e0514a.html>.

[93] North Atlantic Treaty Organization, NATO Parliamentary Assembly, "Article 5," 9-12 June 2008 – Visit To Estonia And Finland - Sub-Committee On Transatlantic Defence And Secuirty Co-Operation, 2008, Web, 22 Mar. 2010 <http://www.nato-pa.int/default.Asp?SHORTCUT=1593>.

[94] "Press Announcement of the CCDCOE - October 28, 2008," CCDCOE, 28 Oct. 2008, Web, 22 Mar. 2010 <http://www.ccdcoe.org/21.html>.

[95] "History and Way Ahead," CCDCOE, 19 June 2009, Web, 22 Mar. 2010 < http://www.ccdcoe.org/12.html>.

5) Providing advice, if asked, during ongoing attacks.[96]

The CCD CoE has "highlighted the development of a good legal framework as 'perhaps the single most pressing need within the domain of computer network defence.'"[97] The main problem with the CCD CoE is that it does not provide immediate assistance to cyber attacks as the CCD CoE is "thought of as a research and learning centre where best practices are developed and shared."[98]

As a complement to the CCD CoE, NATO established the Cyber Defence Management Authority (CDMA) on April 2008, one month prior to the establishment of CCD CoE.[99] The CDMA is a "NATO-wide authority charged with initiating and coordinating 'immediate and effective cyber defence action where appropriate'" for NATO members.[100] On request, the CDMA is able to "coordinate or provide assistance in a concerted effort if an Ally or Allies fall victim to a cyber attack of national or Allied significance."[101] For cyber attacks, the CDMA is the acting body while the CCD CoE is the thinking body.

The CCD CoE and the CDMA are not the only NATO bodies that have important roles in developing and influencing NATO's legal framework on cyber attacks and cyber warfare. The North Atlantic Council maintains control over NATO's policies and activities regarding cyber defense.[102] NATO's Consultation, Control and Command Agency (NC3A) and the NATO Military Authorities (NMA) will implement any new policies; and NATO's Computer

---

[96] North Atlantic Treaty Organization, "027 DSCFC 09 E - NATO and Cyber Defence," Section 45.
[97] Ibid. Section 46.
[98] Ibid.
[99] Ibid. Section 49.
[100] Ibid. Section 47
[101] Ibid.
[102] "Defending Against Cyber Attacks," North Atlantic Treaty Organization, 29 Jan. 2009, Web, 22 Mar. 2010 <http://www.nato.int/issues/cyber_defence/index.html>.

Incident Response Capability (NCIRC) will respond to any cyber aggression against NATO.[103] NATO's goal of establishing a legal framework for cyber attacks would be difficult as NATO's policymakers want to maximize the levels of deterrence against cyber attacks while not limiting their options to respond.[104]

After extensive examination of the Estonian cyber attacks of 2007, Gadi Evron, security specialist for Beyond Security and a leading investigator of the Estonian cyber attacks of 2007, believes that the Estonian cyber attacks came from "flash mobs," a large mass of individual attackers, rather than from Russia's government.[105] He states that "anyone pointing fingers is wrong" when concerning the identities of the attackers for the Estonian cyber attacks of 2007.[106] There is evidence that the first wave of cyber attacks were well organized and that they may have come from a single attacking institute, but Evron discovered that the vast majority of cyber attacks after the first wave were spontaneous and came from different sources, indicating that there were numerous participants.[107] These "flash mobs" were the main instigators for these cyber attacks that lasted for three weeks.[108] Russia's government may still have been responsible for some of these cyber attacks, particularly the first wave of cyber attacks, but to what extent is still unknown.

On an interesting note, Dmitri Galushkevich, a 20-year-old ethnic Russian, became the first individual to be convicted of "cyber war" and be prosecuted for conducting cyber attacks against

---

[103] Ibid.
[104] North Atlantic Treaty Organization, "027 DSCFC 09 E - NATO and Cyber Defence," Section 54.
[105] Robert Vamosi, "Flash mob in Estonia," *Cnet*, N.p., 10 July 2007, Web, 22 Mar. 2010, <http://reviews.cnet.com/4520-3513_7-6761400-1.html?tag=mncol;txt>.
[106] Ibid.
[107] Ibid.
[108] Ibid.

Estonia.[109] Galushkevich was fined 17,500 kroons (1,620 USA dollars) for contributing to the Estonian cyber attacks.[110] He explains that his cyber attacks on the website of Reform Party of Prime Minister Andrus Ansip were for protest.[111] In the grand scheme of the Estonian cyber attacks of 2007 incident, Galushkevich was only a pawn.

IX. The Russia-Georgia Conflict

On August 8, 2008, Russia committed the first cyber war that merged the battlefields of both physical space and cyberspace. The conflict began when Georgia launched a military strike in South Ossetia in attempts to reclaim the territory after sixteen years of semi-independence. In response, Russia attacked Georgia, claiming that Georgia killed Russian peacekeepers and that Georgia was actively committing acts of "ethnic cleansing."[112] Within hours of Russia's initial ground assault, a series of coordinated cyber attacks began attacking, disrupting, and defacing Georgia's websites. However, the first wave of cyber attacks actually began weeks before the Russia-Georgia Conflict. On July 19, 2008, three weeks before the Russia-Georgia Conflict, Georgia's presidential website <www.president.gov.ge> was the target of DDoS attacks, rendering the site unavailable for twenty-four hours.[113] It was believed that these attacks originated from Russia, especially since Russian

---

[109] "Estonia Fines Man for 'Cyber War'," BBC News, 25 Jan. 2008, Web, 22 Mar. 2010 <http://news.bbc.co.uk/2/hi/technology/7208511.stm>.
[110] Ibid.
[111] AFP, "Hacker Convicted in 'Cyber-War.'"
[112] Jeffrey Stinson, "Questions Answered on Russia, Georgia Conflict," USA Today, 8 Aug. 2008, Web, 22 Mar. 2010 <http://www.usatoday.com/news/world/2008-08-08-question-answer_N.htm>.
[113] Dancho Danchev, "Georgia President's Web Site Under DDoS Attack From Russian Hackers," Zero Day Net, 22 July 2008, Web, 22 Mar. 2010 <http://blogs.zdnet.com/security/?p=1533>.

hackers were blamed for pervious cyber attacks that shut down 300 Lithuanian sites with DDoS attacks.[114] These cyber attacks that hit weeks before the Russia-Georgia conflict could have been tests that measured the effectiveness of cyber attacks against Georgia.[115]

According to external monitoring from Shadowserver Foundation, the first DDoS attack hit Georgia at 2:00 PM GMT on August 8, 2008.[116] Throughout the conflict, six different botnets participated in attacking Georgian government and media websites.[117] These cyber attacks shut down the websites of the President of Georgia, the Georgian Parliament, the Ministry of Defense, the Ministry of Foreign Affairs, the National Bank of Georgia, the English-language on-line news dailies "The Messenger," and the English-language on-line news portal <www.civil.ge>.[118] Furthermore, these cyber attacks defaced the Georgian Ministry of Foreign Affairs and the National Bank of Georgia's websites by posting up digitally altered images of President Saakashvilli superimposed over a collage of Adolph Hitler photos.[119] In response to the cyber attacks against Georgia, Estonia and NATO's Cooperative Cyber Defense Center of Excellence (CCD CoE) started to host the websites of Georgian Ministry of Foreign Affairs, National Bank of Georgia, and the website <www.civil.ge>.[120] In addition, Estonia and the CCD CoE

---

[114] Dancho Danchev, "300 Lithuanian Sites Hacked by Russian Hackers." Zero Day Net, 2 July 2008, Web, 10 Jan. 2010 <http://blogs.zdnet.com/security/?p=1408&tag=col1;post-1533>.
[115] Alexander Melikishvili, "The Cyber Dimension of Russia's Attack on Georgia." *Eurasia Daily Monitor*, 11 Sept. 2008, Volum: 5 Issue: 175 sec.: n. pag, Web, 22 Mar. 2010 <http://www.jamestown.org/single/?no_cache=1&tx_ttnews[tt_news]=33936>.
[116] Ibid.
[117] Ibid.
[118] Ibid.
[119] Ibid.
[120] Ibid.

dispatched two information security specialists from its Computer Emergency Response Team (CERT) to help Georgian authorities combat against the cyber attacks.[121]

Furthermore, hours after the initial ground assault, websites and blogs started posting information and tools that allowed users to perform these cyber attacks. These websites encouraged users to partake in the cyber attacks against Georgia. Most notably, a password protected website known as <StopGeorgia.ru> posted hacking tools, detailed instructions, and a list of Georgian websites for visitors to attack during the conflict. [122] This website also hosted a scoreboard that listed all the targeted Georgian websites that were still operational.[123] There were speculations concerning the involvement of the Russian government with <StopGeorgia.ru> due to the website's complexities and the speed at which the website launched, hours after the first ground assault.[124]

On March 20, 2009, a volunteer group of security experts issued a followed-up report named Grey Goose 2 that analyzed the cyber attacks of the Russia-Georgia conflict.[125] The Grey Goose 2 report claimed that Russian intelligence agencies may have been involved in constructing and sponsoring the website <StopGeorgia.ru>.[126] The IP address used for <StopGeorgia.ru> is 75.126.142.110, and the IP address is associated with an Internet

---

[121] Ibid.
[122] Brian Krebs, "Report: Russian Hacker Forums Fueled Georgia Cyber Attacks," The Washington Post, 16 Oct. 2008, 12 Feb. 2009 <http://voices.washingtonpost.com/securityfix/2008/10/report_russian_hacker_forums_f.html>.
[123] Melikishvili, "The Cyber Dimension of Russia's Attack on Georgia."
[124] Krebs, "Report: Russian Hacker Forums Fueled Georgia Cyber Attacks."
[125] Robert McMillan, "Report Links Russian Intelligence to Cyber Attacks," IT World, 20 Mar. 2009, Web, 22 Mar. 2010 <http://www.itworld.com/security/64751/report-links-russian-intelligence-cyber-attacks>.
[126] Ibid.

service provider (ISP) called SteadyHost <www.steadyhost.ru>."[127] SteadyHost has offices in an apartment building at 88 Khoroshevskoe Shosse, Moscow. [128] The "Center for Research of Military Strength of Foreign Countries" and the GRU are located at 86 Khoroshevskoe Shosse and at 76 Khoroshevskoe Shosse respectively, literally a city block down from the offices of SteadyHost.[129] The Grey Goose 2 report concluded the following:

> In the case of possible Russian government involvement with the cyber attacks on Georgian government websites in July and August, 2008, the available evidence supports a strong likelihood of GRU/FSB planning and direction at a high level while relying on Nashi[130] intermediaries and the phenomenon of crowdsourcing to obfuscate their involvement and implement their strategy.[131]

The report's principal author, Jeff Carr, believes that "there's just too much planning that went into it [cyber attacks]" for the attacks not to be associated with Russia's government.[132]

X. The Predicaments and Problems with the UN's Legal Framework for Cyber Attacks

---

[127] Jeff Carr, Project Grey Goose Phase II Report: The Evolving State of Cyber Warfare, 2008, Comp. Billy Rios, et al, Ed. Derek Plansky and Kristan Wheaton, 2nd ed. 2009, 16, Greylogic, 20 Mar. 2009, Web, 22 Mar. 2010 <http://www.scribd.com/doc/13442963/Project-Grey-Goose-Phase-II-Report>.
[128] Ibid. 17.
[129] Ibid.
[130] From Grey Goose Phase II report: Also known as, "Youth Democratic Anti-Fascist Movement 'Ours!'" Nashi is a hacking group that may be receiving government funding. One of the main supporters is Vladislav Surkov, the First Deputy Chief of the Presidential Staff.
[131] Carr, Project Grey Goose Phase II Report: The Evolving State of Cyber Warfare, 5.
[132] McMillan, "Report Links Russian Intelligence to Cyber Attacks."

During the Russia-Georgia conflict, websites and blogs posted programs, methods, and a list of websites for visitors to attack Georgia's networks. In the article "An Army of Ones and Zeroes: How I became a soldier in the Georgia-Russia Cyberwar," Evgeny Morozov describes his experience in enlisting as a cyber soldier in the cyber war against Georgia.[133] After a quick online search, Morozov discovered a blog that informed him of a method to refresh Georgian web pages continuously within a single window, flooding the website with thousands of queries per minute.[134] Next, he created a simple .BAT extension file, which he dubbed an "e-Molotov," that was capable of sending thousands of ping requests per second with a simple double-click of the file.[135] Finally, he concluded his research by visiting <StopGeorgia.ru> and found a software utility named DoSHTTP, which allowed a user to attack a targeted website by just clicking the user-friendly "Start Flood" button, essentially allowing "war at the touch of a button."[136]

Morozov is just one of many users who contributed to the cyber attacks against Georgia during the Russia-Georgia conflict. The sheer number of participants during the Russia-Georgia conflict helped mask the "footprints" of the main instigator for these cyber attacks. The participants include hacktivists (political activist hackers)[137], "script-kiddies" (derogatory term for "immature" hackers)[138], and botnets that vastly obfuscate the main attackers'

---

[133] Evgeny Morozov, "An Army of Ones and Zeroes: How I became a soldier in the Georgia-Russia Cyberwar," Slate, 14 Aug. 2008, Web, 22 Mar. 2010 <http://www.slate.com/id/2197514/pagenum/all/>.
[134] Ibid.
[135] Ibid.
[136] Ibid.
[137] "Hacktivism," SearchSecurity, 05 Jun. 2007, Web, 22 Mar. 2010 <http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci552919,00.html>.
[138] "Script Kiddy," SearchSecurity, 11 Mar. 2009, Web, 22 Mar. 2010 <http://searchmidmarketsecurity.techtarget.com/sDefinition/0,,sid198_gci550928,00.html>.

involvement with cyber attacks.[139] For the Russia-Georgia Conflict, there is evidence that the Russian government was involved in aiding participants in performing cyber attacks by hosting the website <StopGeorgia.ru>. However, for future cyber attacks, it will be difficult, if not impossible, to identify the main attacker. The only solution to this problem is the continual development and improvement of international cyber law enforcement groups and tracing programs.

What happens if a non-NATO country is attacked with cyber attacks? Georgia, unlike Estonia, is not a member of NATO. NATO committed itself in extending NATO alliance membership to Georgia, as discussed in Article 23 during the April 2008 Bucharest Summit meeting.[140] Unfortunately, all discussions concerning Georgia's membership to NATO ceased when Russia attacked Georgia. Georgia may not have been a NATO member, but Georgia is a UN member, and has been one since July 31, 1992.[141] Georgia must rely on the UN Charter and the UN's legal framework to handle these cyber attacks. For the Russia-Georgia conflict, the UN can easily intervene since the cyber attacks included a physical invasion.

What if Russia attacked Georgia only with cyber attacks, in a similar manner to the Estonian cyber attacks of 2007? How would the UN Charter handle cyber attacks that had no components of physical attacks? With this supposition, the following will be an examination of how the UN Charter will handle a continual barrage of cyber attacks, such as the case of the Estonian cyber attacks of 2007. The UN Charter "forbids 'acts of aggression' and restricts 'the

---

[139] Carr, Project Grey Goose Phase II Report: The Evolving State of Cyber Warfare, 5.
[140] Bucharest Summit Declaration: 3 April 2008, "Article 23."
[141] "Member States of the United Nations," United Nations, 3 July 2006, Web, 22 Mar. 2010 <http://www.un.org/en/members/index.shtml#g>.

threat or use of force' in peacetime" [UN charter: Art. 1, Para. 1; and Art. 2, Para. 4] while ensuring the "inherent right of individual or collective self-defence if an *armed attack* occurs against a Member of the United Nations"[142][Italics added for emphasis] under Article 51.[143] Other factors that determine a certain action as being an "act of force" is the action's expected lethality, destructiveness, and invasiveness.[144] Most importantly, methods of economic sanctions and actions of interrupting communications do not constitute a "use of force" under the UN Charter.[145] If Article 41 is coupled with Article 2, paragraph 4: "All Members shall refrain in their international relations from the threat or *use of force* against the territorial integrity or political independence of any state,"[146][Italics added for emphasis] then it creates a situation that non-lethal, non-destructive, and non-invasive information operations that interrupt communications may be permissible under the charter.[147] If Article 41 declares that disrupting communications is not a "use of force," then it can be easily inferred that cyber attacks that disrupt communications are not a "use of force."

The UN Charter has two main problems when addressing cyber attacks. The first problem is that according to Article 2 and Article 41 of the UN Charter, cyber attacks may be permissible, or at the least not prohibitive, when they are used as a means of disrupting

---

[142] United Nations, Chapter VII: Action with Respect to Threats to the Peace, Breaches of the Peace, and Acts of Aggression, Article 51, Web, 22 Mar. 2010 <http://www.un.org/en/documents/charter/chapter7.shtml>.
[143] Grove, G. D., S. E. Goodman, and S. J. Lukasik. "Information Operations and the UN Charter," Cyber-Attacks and International Law, Survival, 2000. Vol. 42. 3.: 93.
[144] Ibid.
[145] Ibid. 93-94.
[146] United Nations, Chapter 1: Purposes and Principles, Article 2, Web, 22 Mar. 2010 <http://www.un.org/en/documents/charter/chapter1.shtml>.
[147] Grove 93.

a country's communications. Coupled with the fact that attacks on communications or economic sanctions are not a "use of force," the UN would have been legally powerless in stopping cyber attacks. The second problem is that the UN Charter does not specify the appropriate response for cyber attacks. If state-sponsored cyber attacks are signs of aggression, then the UN Charter needs to reflect this stance by classifying cyber attacks as armed attacks and a "use of force." Furthermore, there needs to be transparent guidelines for describing an appropriate response to state-sponsored cyber attacks. Currently, there is ambiguity concerning the appropriate response that a country can give if it is a victim of cyber attacks. Should a victimized country of state-sponsored cyber attacks be allowed to respond with counter cyber attacks or an actual physical counterattack? Similar to NATO, the UN needs to define the rights for the victimized country of cyber attacks.

The Russia-Georgia conflict showed how problematic the UN Charter is in dealing with cyber attacks. Currently, NATO is further along in their development of a legal framework for cyber attacks than the UN. During the Russia-Georgia conflict, NATO, unlike the UN, was willing to host Georgia's websites and to aid Georgia by providing two information security specialists.[148] Georgia is not a part of NATO, yet NATO was willing to extend resources to help Georgia defend against Russia. Based solely on actions, NATO is more adept at responding to cyber attacks than UN. The UN still has a long way in their development of an international legal framework for cyber attacks, especially when detailing the rights for a victimized country of cyber attacks.

XI. The GhostNet Incident

On March 29, 2009, a research group known as the Information Warfare Monitor (IWM) released their report "Tracking

[148] Melikishvili, "The Cyber Dimension of Russia's Attack on Georgia."

Ghostnet: Investigating a Cyber Espionage Network."[149] This report investigated the cyber espionage incident of the Tibetan community during June 2008 to March 2009.[150] IWM documented evidence of a program called GhostNet that penetrate and infect the computer systems of the private offices of the Dalai Lama and other Tibetan targets. Furthermore, IWM discover that GhostNet infected 1,295 computers in 103 countries, of which 30% of the infected computers are considered high-value diplomatic, political, economic, and military targets.[151] The targets include:

> Foreign ministry affairs of Iran, Bangladesh, Latvia, Indonesia, Philippines, Brunei, Barbados, and Bhutan; embassies of India, South Korea, Indonesia, Romania, Cyprus, Malta, Thailand, Taiwan, Portugal, Germany and Pakistan; the ASEAN (Association of Southeast Asian Nations) Secretariat, SAARC (South Asian Association for Regional Cooperation), and the Asian Development Bank; news organizations; and an unclassified computer located at NATO headquarters.[152]

GhostNet involves a program named "gh0st RAT" which allows an attacker to have complete, real-time control of an infected system.[153] GhostNet allows the attacker to search and remove files from a system, log keystrokes, screen capture, and silently activate web cameras and audio inputs without the target's knowledge. [154] [155] GhostNet spreads through contextually relevant e-mails that are

---

[149] Greg Walton and Nart Villenueve, Tracking GhostNet: Investigating a Cyber Espionage Network, Comp, Ronald Deibert, et al. 2009, 28 Mar. 2009,: 1, Web, 22 Mar. 2010 <http://www.scribd.com/doc/13731776/Tracking-GhostNet-Investigating-a-Cyber-Espionage-Network>.
[150] Ibid. 11.
[151] Ibid. 7.
[152] Ibid. 6.
[153] Ibid.
[154] Ibid. 39
[155] Ibid. 47

laced with the program. Once a system is infected, GhostNet allows the attacker to scan the infected system's contacts list and to send out e-mails laced with this malicious program to the contacts.[156] Based on how GhostNet spreads, the authors of the report believe that the inclusion of high value targets were coincidental.[157] There are speculations concerning China's involvement with GhostNet, especially since there is evidence that gh0st RAT is being controlled from commercial Internet access accounts located in Hainan, People's Republic of China. However, the Hainan proxy computers may have been controlled by another country or group to mislead investigators.[158] As for this writing, neither the purpose nor the perpetrators of GhostNet have been discovered.

XII. GhostNet and Apolo Ohno Controversy: The Gray Boundaries of Aggression

If NATO, the UN, and other alliances are establishing laws and preventive measurements for state-sponsored cyber attacks, then each alliance would need to draw a legal line in the grey legal boundaries of cyber attacks. GhostNet presents an elaborated and frightening reality of a massive cyber espionage operation, with the primary target being the Dalia Lama networks. The sole existence of GhostNet is to allow an attacker to have complete, anonymous, and secretive control over all the targeted computers' information. If GhostNet is capable of searching and deleting files, then it is capable of altering the function of key programs and wiping out all data on a hard drive. Furthermore, the spread of GhostNet was not done through "front door" methods of cyber attacks; rather, it was done through recipients opening up contextually relevant e-mails laced with infected files that automatically install GhostNet onto their systems. With this in mind, how should laws be crafted to handle

[156] Ibid. 5-6
[157] Ibid. 6
[158] Ibid. 49

this type of cyber attack? Should this type of cyber attack be considered a form of espionage and treated as a cyber attack? What happens if spies were to be involved in installing this program deeper into the targeted government's networks? To craft an effective international legal framework for cyber threats, governments and alliances need to be aware of all the capabilities of cyber attacks and the methods of attacks. A legal framework needs to be wide scoped to encompass all the different uses of cyber attacks while still being detail oriented in listing appropriate responses for different cyber attacks.

When developing the legal framework for cyber attacks, governments and alliances need to consider the intent and the potential harm of cyber attacks. The GhostNet incident has unimaginable spying and destructiveness capabilities. Yet cyber attacks may have another purpose, as evident with the Apolo Ohno controversy. The Apolo Ohno controversy presents a unique case of a country allegedly conducting cyber attacks as a sign of protest.[159] During the 2002 Salt Lake City Winter Olympics, Apolo Ohno was awarded the gold medal in the 1,500-meter-speed-skating race after South Korea's skater Kim Dong-Sung was disqualified.[160] Hours after this upset, a series of DDoS attacks most likely originating from South Korea hit several United States-based servers, possibly as a response to this disqualification.[161] If the cyber attacks did come from South Korea, then the Apolo Ohno incident can be considered a politically based cyber attack. Instead of voicing political outcries over the disqualification of Kim Dong-Sung, South Korea's

---

[159] Robert Vamosi, "Newsmaker: Cyberattack In Estonia--What It Really Means," Cnet News, 29 May 2007, Web, 22 Mar. 2010 <http://news.cnet.com/Cyberattack-in-Estonia-what-it-really-means/2008-7349_3-6186751.html?tag=untagged>.
[160] Ibid.
[161] Ibid.

government or South Korean citizens may have conducted the cyberspace equivalent of a political "jab."

Cyber attacks have become more than weapons of modern warfare; they are political tools for governments. Cyber attacks can be used for both destructive and political purposes. But what propels a government to carry out cyber attacks, whether for political or destructive reasons? Governments may be conducting state-sponsored cyber attacks for this sole reason: because they can. Due to a cyber attack's anonymous nature, any government that conducts cyber attacks has de facto plausible deniability. State-sponsored cyber attacks can be viewed as government's a display of power. Instead of solving issues through physical channels, governments can now use cyber attacks as powerful political tools for "silent" and anonymous attacks to either bully or retaliate against past transgressions.

How should international legal frameworks for cyber attacks be crafted to encompass the destructive nature of Estonia and Georgia's cyber attacks, the cyber espionage of GhostNet, and the political tools employed for the Apolo Ohno controversy? Where should the legal line be drawn within the grey legal boundaries of cyber attacks? These discussions are happening more frequently amongst governments and alliances as they acknowledge that current laws are not adequate for this growing threat. However, developing the appropriate legal framework for cyber attacks is not enough. From all these cyber attack incidents, one thing stands out: the law is too slow in addressing these cyber attacks. The development of better cyber security and international cyber law enforcements groups are as important, if not more important, than the development of the legal framework for cyber attacks and cyber warfare.

XIII. Conclusion

The current international legal frameworks for cyber attacks, whether concerning the legal foundation or the responses to cyber

attacks, are inadequate for addressing the full capabilities of cyber attacks. The research throughout this paper indicates that governments and alliances are having great difficulties in defining the rights for the victimized country of cyber attacks. The following is a brief recap of what was discussed through the course of this paper: the current legal problems of cyber attacks, the inherent problems of the Internet which promote cyber attacks, the different methods of cyber attacks, the goals for a developing international legal framework for cyber attacks, the current development of NATO's legal framework for cyber attacks as a response to the Estonian cyber attacks of 2007, the problems within the UN Charter for controlling cyber attacks, and the problem of establishing the legal line within the gray boundaries of cyber attacks.

Questions concerning the future development of the legal framework for cyber attacks are: should cyber espionage be treated the same as destructive cyber attacks? What differentiates an attacker from an unwilling participant of cyber attacks? Should social engineering be treated legally the same as physical spying and reconnaissance? How should a country respond to a known state-sponsored cyber attack? Should there be any form of response or punishment after determining the attacker of a cyber attack, even if this information is found months or years after the attacks? Are cyber attacks considered armed attacks or use of force? What are the rights for the victimized country of cyber attacks?

The main advantage to having an international legal framework for cyber attacks is that it establishes communication protocols that allow governments and alliances to discuss cyber attacks in a proper forum. These discussions can establish levels of acceptability for cyber attacks, increase political and public awareness of cyber attacks and cyber warfare, and promote the growth of newer and better technology for cyber security. Furthermore, these discussions allow for governments and alliances to determine the directions that international legal frameworks

should head towards. Currently, both United States and Russia have contrary viewpoints for how the overarching international legal framework for cyber attacks should be developed. The United States wants an international legal framework that favors international law enforcement groups handling cyber attacks.[162] Conversely, Russia desires an international treaty addressing cyber attacks.[163] The reason that the United States favors international law enforcement groups is that it already has these enforcement groups established through NATO, particularly the CCD CoE and CDMA. Since Russia does not have its own law enforcement groups, Russia favors an international treaty. However, an international treaty with Russia may be disadvantageous for the United States and other countries since Russia is one of the biggest offenders of state-sponsored cyber attacks. Potentially, Russia could create an international treaty that may permit them or other countries to conduct certain types of cyber attacks. It is dangerous to put so much faith into an international treaty, especially since cyber attacks will still happen with or without an international treaty. Strengthening international law enforcement groups would allow for rapid responses and prosecution against cyber attacks.

An international legal framework consisting only of international legal instruments and bilateral agreements would be futile for stopping the cyber attacks for this sole reason: there are no rules or boundaries in cyber space. For cyber attacks, anything can happen and will happen. An international legal framework needs international law enforcement groups. As governments and alliances become involved with combating cyber attacks, advancements in

---

[162] John Markoff and Andrew E. Kramer, "U.S. and Russia Differ on a Treaty for Cyberspace." *The New York Times*, 27 June 2009: 1-2. Web, 22 Mar. 2010 <http://www.nytimes.com/2009/06/28/world/28cyber.html?_r=4&pagewanted=1>.

[163] Ibid.

technology will lead to better cyber security and enforcement tools for these international law enforcement groups. However, cyber security and international law enforcement groups will not prevent cyber attacks from happening for this sole reason: there is no perfect defense for cyber security. Governments and alliances need an international legal framework that does two things: one, to be able to define and establish globally accepted laws, procedures, and punishments for cyber attacks; and two, to be able to enforce, to respond to, and to prosecute these cyber attacks efficiently. Legally, an international legal framework provides governments and alliances communication protocols to discuss cyber attacks and cyber warfare. Practically, an international legal framework creates and establishes international law enforcement groups and global standards of cyber security that prevent, respond, investigate, and identify state-sponsored cyber attacks. Out of all the research done for this paper, one thing is certain: cyber attacks and cyber warfare will continue to happen, with or without an international legal framework.

Works Cited

AFP. "Hacker Convicted In 'Cyber-War.'" FRANCE 24. 23 Jan. 2008. Web. 22 Mar. 2010 <http://www.france24.com/en/20080123-hacker-convicted-cyber-war-estonia-justice>.

AFP. "Hackers harpoon executives in 'whaling' attacks." The Sydney Morning Herald. 6 May 2008. Web. 22 Mar. 2010 <http://www.smh.com.au/news/security/hackers-harpoon-executives-in-whaling-attacks/2008/05/06/1209839606696.html>.

Barnes, Julian E. "Pentagon Computer Networks Attacked." *Los Angeles Times* 28 Nov. 2008: 1-3. Web. 22 Mar. 2010. <http://articles.latimes.com/2008/nov/28/nation/na-cyberattack28>.

"Botnet." SearchSecurity. 30 Oct. 2008. Web. 22 Mar. 2010 <http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci1030284,00.html>.

"Bots and Botnets— A Growing Threat." Norton from Symantec. Web. 22 Mar. 2010 <http://www.symantec.com/norton/theme.jsp?themeid=botnet>.

"Bucharest Summit Declaration." NATO. 3 Apr. 2008. Web. 22 Mar. 2010 <http://www.nato.int/cps/en/natolive/official_texts_8443.htm>.

Carr, Jeff. Project Grey Goose Phase II Report: The Evolving State of Cyber Warfare. 2008.

Comp. Billy Rios, et al. Ed. Derek Plansky and Kristan Wheaton. 2nd ed. 2009. Greylogic. 20 Mar. 2009. Web. 22 Mar. 2010

<http://www.scribd.com/doc/13442963/ Project-Grey-Goose-Phase-II-Report>.

Coleman, Kevin. "China Hacks White House Email?" DefenseTech. Ed. Christian Lowe. 11 Nov. 2008. Military. Web. 22 Mar. 2010 <http://www.defensetech.org/archives/004524.html>.

"Conficker: FAQ." Conficker Working Group. 26 Mar. 2009. Web. 22 Mar. 2010 <http://www.confickerworkinggroup.org/wiki/pmwiki.php/ANY/FAQ>.

"Conficker: Timeline." Conficker Working Group. 26 Apr. 2009. Web. 22 Mar. 2010 <http://www.confickerworkinggroup.org/wiki/pmwiki.php/ANY/Timeline>.

"Convention on Cybercrime CETS No.: 185." *Council of Europe*. N.p., 4 Jan. 2010. Web. 9 Jan. 2010. <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=04/01/2010&CL=ENG>.

Danchev, Dancho. "300 Lithuanian Sites Hacked by Russian Hackers." *ZDNet*. CBS Interactive Inc., 2 July 2008. Web. 22 Mar. 2010. <http://blogs.zdnet.com/security/?p=1408&tag=col1;post-1533>.

Danchev, Dancho. "Georgia President's Web Site under DDoS Attack from Russian Hackers." Zero Day Net. 22 July 2008. Web. 22 Mar. 2010 <http://blogs.zdnet.com/security/?p=1533>.

"Defending Against Cyber Attacks." North Atlantic Treaty Organization. 29 Jan. 2009. Web. 22 Mar. 2010 <http://www.nato.int/issues/cyber_defence/index.html>.

Drupal. "Use Of Botnets." The Honeynet Project. 10 Aug. 2008. Web. 22 Mar. 2010 <http://www.honeynet.org/node/52>.

"Estonia Fines Man for 'Cyber War'." BBC News. 25 Jan. 2008. Web. 22 Mar. 2010 <http://news.bbc.co.uk/2/hi/technology/7208511.stm>.

Estonia. Cyber Security Strategy Committee. "3.4.1. International Law." *Cyber Securit Strategy*. *Estonian Ministry of Defence*. N.p., 2008. Web. 23 Mar. 2010. <http://www.mod.gov.ee/files/kmin/img/files/Kuberjulgeoleku_strateegia_2008-2013_ENG.pdf>. [PDF file accessed from English version of Estonian Ministry of Defence, National Defense and Society: Cyber Security <http://mod.gov.ee/en/national-defense-and-society> (Last updated 23 Mar. 2010)]

Grove, Gregory D., Seymour E. Goodman, and Stephen J. Lukasik. "Information Operations and the UN Charter." Cyber-Attacks and International Law. 2000. Vol. 42. 3.: 89-104.

"Hacktivism." SearchSecurity. 05 Jun. 2007. Web. 22 Mar. 2010 <http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci552919,00.html>.

"History And Way Ahead." CCDCOE. 19 June 2008. Web. 22 Mar. 2010 <http://www.ccdcoe.org/12.html>.

Howe, Walt. "A Brief History of the Internet." Walt Howe's Internet Learning Center. 1 Sept. 2009. Web. 22 Mar. 2010 <http://www.walthowe.com/navnet/history.html>.

Krebs, Brian. "Report: Russian Hacker Forums Fueled Georgia Cyber Attacks." The Washington Post. 16 Oct. 2008. Web. 22 Mar. 2010 <http://voices.washingtonpost.com/securityfix/2008/10/report_russian_hacker_forums_f.html>.

Leyden, John. "Estonian/Russian statue riots spill online." The Register. 1 May 2007. Web. 22 Mar. 2010 <http://www.theregister.co.uk/2007/05/01/estonian_riots/>.

Lipson, Howard F., Ph.D. Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues. Ed. Pamela Curtis and Mindi McDowell. Springfield: U.S. Department of Commerce, 2002. Nov. 2002. CERT® Coordination Center. Web. 22 Mar. 2010 <www.cert.org/archive/pdf/02sr009.pdf>.

Lobjakas, Ahto. "News Analysis: How Vulnerable Are Countries To Cyberattacks? Ask Estonia!." Radio Free Europe/Radio Liberty. 29 Apr. 2008. Web. 22 Mar. 2010 <http://www.rferl.org/content/Article/1109653.html>.

"Marching Off To Cyberwar." The Economist 4 Dec. 2008. Technology Quarterly. Web. 22 Mar. 2010 <http://www.economist.com/science/tq/displaystory.cfm?story_id=12673385>.

Markoff, John, and Andrew E. Kramer. "U.S. and Russia Differ on a Treaty for Cyberspace." *The New York Times* 27 June 2009: 1-2. Web. 22 Mar. 2010.

<http://www.nytimes.com/2009/06/28/world/28cyber.html?_r=4&pagewanted=1>.

McMillan, Robert. "Report Links Russian Intelligence to Cyber Attacks." IT World. 20 Mar. 2009. Web. 22 Mar. 2010 <http://www.itworld.com/security/64751/report-links-russian-intelligence-cyber-attacks>.

Melikishvili, Alexander. "The Cyber Dimension of Russia's Attack on Georgia." *Eurasia Daily Monitor* 11 Sept. 2008, Volum: 5 Issue: 175 sec.: n. pag. Web. 22 Mar. 2010. <http://www.jamestown.org/single/?no_cache=1&tx_ttnews[tt_news]=33936>.

Mikkelsen, Randall. "U.S. not ready for cyber attack." Reuters. 19 Dec. 2008. Web. 22 Mar. 2010 <http://www.reuters.com/article/domesticNews/idUSTRE4BI00520081219>.

Morozov, Evgeny. "An Army of Ones and Zeroes: How I Became a Soldier in the Georgia-Russia Cyberwar." Slate. 14 Aug. 2008. Web. 22 Mar. 2010 <http://www.slate.com/id/ 2197514/pagenum/all/>.

Neal, David. "Security attacks reach 2.5 billion per day." Vnunet. 5 Dec. 2008. Web. 22 Mar. 2010 <http://www.vnunet.com/vnunet/news/2232104/ibm-boosts-security-services>.
"NATO Opens New Centre of Excellence on Cyber Defence." NATO. 20 May 2008. North Atlantic Treaty Organization. Web. 22 Mar. 2010 <http://www.nato.int/docu/update/2008/05-may/e0514a.html>.

North Atlantic Treaty Organization. "Article 5." The North Atlantic Treaty: 4 April 1949. Washington D.C., 1949. On-Line Library. 29 Nov. 2007. Web. 22 Mar. 2010 <http://www.nato.int/docu/basictxt/treaty.htm>.

North Atlantic Treaty Organization. Bucharest Summit Declaration: 3 April 2008. Bucharest, 2008. 16 Mar. 2009. Web. 22 Mar. 2010 <http://www.nato.int/docu/pr/2008/p08-049e.html>.

North Atlantic Treaty Organization. NATO Parliamentary Assembly. "027 DSCFC 09 E - NATO and Cyber Defence." 2009 Spring Session. Sverre Myrli. NATO Committee Reports. Web. 22 Mar. 2010 <http://natopa.ibicenter.net/default.asp?SHORTCUT=1782>.

North Atlantic Treaty Organization. NATO Parliamentary Assembly. "Article 5." 9-12 June 2008 – Visit to Estonia and Finland - Sub-Committee On Transatlantic Defence and Security Co-Operation. 2008. Web. 22 Mar. 2010 <http://www.nato-pa.int/default.Asp?SHORTCUT=1593>.

"Press Announcement of the CCDCOE - October 28, 2008." CCDCOE. 28 Oct. 2008. Web. 22 Mar. 2010 <http://www.ccdcoe.org/21.html>.

Poulsen, Kevin. "Threat Level Privacy, Crime and Security Online 'Cyberwar' and Estonia's Panic Attack." Threat Level. 22 July 2007. Wired. Web. 22 Mar. 2010 <http://www.wired.com/threatlevel/2007/08/cyber-war-and-e/>.

"Script Kiddy." SearchSecurity. 11 Mar. 2009. Web. 22 Mar. 2010 <http://searchmidmarketsecurity.techtarget.com/sDefinition/0,,sid198_gci550928,00.html>.

"Spear Phishing and Whaling Attacks Reach Record Levels." iDefense Labs. 7 June 2008. Web. 22 Mar. 2010 <http://labs.idefense.com/news/press/bbb/>.

Stinson, Jeffrey. "Questions Answered on Russia, Georgia Conflict." USA Today. 8 Aug. 2008. Web. 22 Mar. 2010 <http://www.usatoday.com/news/world/2008-08-08-question-answer_N.htm>.

"The Cyber Raiders Hitting Estonia." BBC News. 17 May 2007. Web. 22 Mar. 2010 <http://news.bbc.co.uk/2/hi/europe/6665195.stm>.

"The Warnings?" Cyber War! 24 Apr. 2003. Frontline, PBS. Web. 22 Mar. 2010 <http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/warnings/>.

Traynor, Ian. "Russia Accused of Unleashing Cyberwar to Disable Estonia." Guardian News and Media Limited. 17 May 2007. Web. 22 Mar. 2010 <http://www.guardian.co.uk/world/2007/may/17/topstories3.russia>.

United Nations. Chapter 1: Purposes and Principles. Article 2. Web. 22 Mar. 2010 <http://www.un.org/en/documents/charter/chapter1.shtml>.

United Nations. Chapter VII: Action with Respect to Threats to the Peace, Breaches of the Peace, and Acts of Aggression. Article 51. Web. 22 Mar. 2010 <http://www.un.org/en/documents/charter/chapter7.shtml>.

United States. Cong. The NATO Summit at Bucharest, 2008. By Paul Gallis. The Library of Congress, 2008. CRS Report for Congress. Web. 22 Mar. 2010. Congressional Research Service. 22 Mar. 2010 <http://www.fas.org/sgp/crs/row/RS22847.pdf>.

Vamosi, Robert. "Flash mob in Estonia." *Cnet*. N.p., 10 July 2007. Web. 22 Mar. 2010. <http://reviews.cnet.com/4520-3513_7-6761400-1.html?tag=mncol;txt>.

Vamosi, Robert. "Newsmaker: Cyberattack in Estonia--What it Really Means." Cnet News. 29 May 2007. Web. 22 Mar. 2010 <http://news.cnet.com/Cyberattack-in-Estonia-what-it-really-means/2008-7349_3-6186751.html?tag=untagged>.

Walton, Greg, and Nart Villenueve. Tracking GhostNet: Investigating a Cyber Espionage Network. Comp. Ronald Deibert, et al. 2009. 1. 28 Mar. 2009. Web. 22 Mar. 2010 <http://www.scribd.com/doc/13731776/Tracking-GhostNet-Investigating-a-Cyber-Espionage-Network>.

White, Greg, et al. CompTIA Security+ All-In-One Exam Guide, Second Edition. 2nd ed. N.p.: McGraw-Hill Companies, 2009.

Conceding the Constitution: How the Intelligence Oversight Act of 1980 aided the Executive

By Mikhail Guttentag

Introduction

For Congress, enacting effective intelligence oversight is an arduous task. Stansfield Turner, who served as the Director of Central Intelligence from 1977-1981, asserts that "there is no easy way to balance the need for sufficient oversight by the Congress in order to ensure a degree of accountability with the intelligence agencies' need to gather and protect the information they require to perform their function."[164] Nevertheless, the Intelligence Oversight Act of 1980 represented, at its most basic level, a Congress determined to stay informed of intelligence activity. Yet if "the nature of intelligence oversight disputes between Congress and the Executive is that of competing claims to constitutional power,"[165] any meaningful evaluation of the 1980 Act requires analyzing how it affected the balance of powers in policing and authorizing intelligence activity. In *Imbalance of Powers: Constitutional Interpretation and the Making of American Foreign Policy*, Gordon Silverstein concludes that in passing the 1980 Act, "Congress' attempt to control the executive's actions in foreign policy only provided fresh and unprecedented explicit authorization for executive prerogative."[166] In assessing this claim, I engage in both historical and textual analysis of the 1980 Act. First, I examine the 1980 Act in its historical context, and show to what extent the political process affected the language of the 1980 Act. Second, I turn to dissect the text of the 1980 Act, and highlight some of the ambiguities and loopholes therein that might lend support to

---

[164] Turner, Stansfield S. *Secrecy and Democracy: the CIA in Transition*. New York, NY: Perennial Library, 1986. Print. 4.

[165] Colton, David. "Speaking Truth to Power: Intelligence Oversight in An Imperfect World." University of Pennsylvania Law Review 137.2 (1988): 571-613. Print. 587.

[166] Silverstein, Gordon. *Imbalance of Powers: Constitutional Interpretation and the Making of American Foreign Policy*. New York: Oxford University Press, 1997. Print. 145.

Silverstein's conclusion. Finally, I look to subsequent interpretations of the 1980 Act–specifically during the Iran-Contra Affair in 1986–to examine to what extent the 1980 Act affected the balance of powers in overseeing covert activity. In doing so, I conclude that while the 1980 Act did broaden reporting requirements to Congress, its ambiguities left the Executive Branch free to expand its autonomy in intelligence activity and evade the oversight Congress hoped to establish.

Placing the 1980 Act in its Historical Context

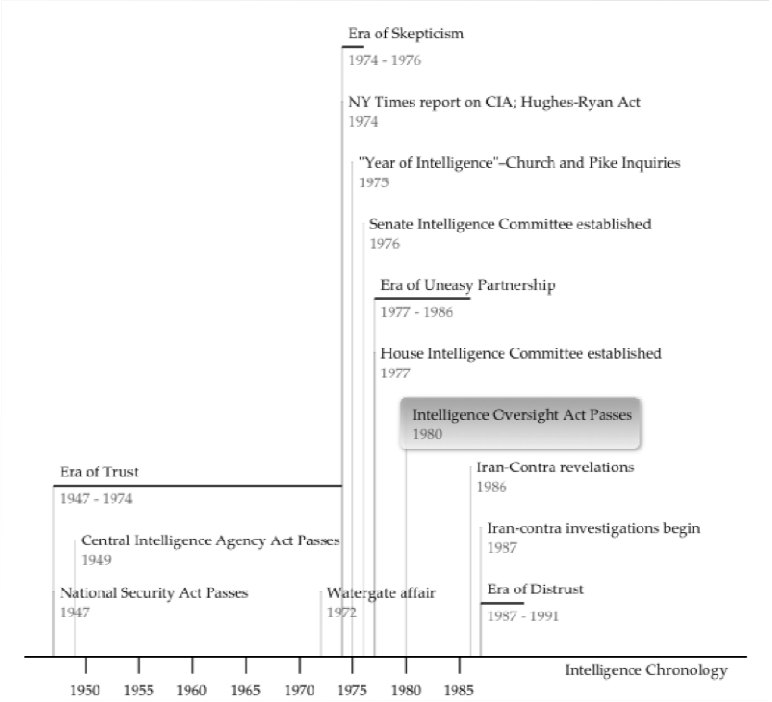


Figure 1 - Intelligence Oversight Timeline (Adapted from Loch Johnson's "Chronology" in *America's Secret Power*).

In analyzing the historical context from which the Intelligence Oversight Act of 1980 arose, Loch K. Johnson placed

the relationship between Congress and the intelligence agencies into three eras: the Era of Trust, lasting from 1947-1974; the Era of Skepticism, lasting from 1974-1976; and the Era of Uneasy Partnership, lasting 1976-1986.[167] Using those three eras as our framework, we can develop a better idea of where the 1980 Act fits in the larger relationship of Congress and its historical oversight of intelligence activity. In addition, the primary accounts of Johnson, who served on the Senate committee investigating the intelligence agencies in 1975, and Stansfield, who headed the Central Intelligence Agency (CIA) during the 1980 Act's passage, shed light on how the 1980 Act was written and received, respectively. In addition, placing the 1980 Act in its historical context allows us to examine two important questions: What role did the public play in Congress' pursuit of stronger intelligence oversight? And, more importantly, what were the objectives of the 1980 Act?

A. Oversight during the Era of Trust (1947-1974): Little Payoff, Little Action

After voting to establish the CIA in the National Security Act of 1947, Congress in the next period of nearly three decades declined to engage in frequent and investigative intelligence oversight. Though the Armed Services and Appropriations Committees held oversight responsibility for the CIA, "the committees–and the Congress as a whole–were lax in carrying out these duties."[168] Johnson quotes Professor Harry Ransom, who characterized congressional oversight over these decades as

---

[167] Johnson, Loch K. *America's Secret Power: the CIA in a Democratic Society*. New York, NY: Oxford University Press, Inc., 1989. Print. Xxiii-xxiv.

[168] McCormick, James, and Steven Smith. "The Iran Arms Sale and the Intelligence Oversight Act of 1980." PS 20.1 (1987): 29-37. Print. 29.

"sporadic, spotty and essentially uncritical."[169] Johnson and other scholars have proposed a number of reasons for Congress' lack of action during these eras. One reason Johnson posits is that Congress may have been frozen with "paralyzing awe engendered by the sheer size and complexity of the intelligence community, with its more than forty agencies and multibillion-dollar expenditures."[170] For this reason, some members of Congress concluded that leaders of intelligence agencies were "honorable men who could be relied upon to do the right thing,"[171] whose jobs would be encumbered by outsiders with little experience in espionage. Another concern had to do with preserving secrecy– Johnson quotes a Senator explaining that the difficulty with asking questions "is that we might obtain information which I personally would rather not have, unless it was essential for me as a member of Congress to have it."[172]

While these reasons all serve as plausible explanations, at least in part, for why Congress did not actively engage in comprehensive intelligence oversight, a study conducted by Bert Rockman examining when and why Congress engages in oversight yields a more plausible explanation for why Congress declined to act: a general lack of a political payoff. As Rockman explains, members of Congress are rational political actors, and "allocate their own limited resources of time and energy to activities that are salient to their own preferential and political interests."[173] Reelection prospects did not hinge on intelligence oversight; as Johnson observes, "legislators are unable to even talk about their

---

[169] Johnson, Loch K. *A Season of Inquiry: the Senate Intelligence Investigation.* Lexington, KY: The University Press of Kentucky, 1985. Print. 8.
[170] Ibid. 7.
[171] Ibid. 7.
[172] Ibid. 8.
[173] Rockman, Bert. "Legislative-Executive Relations and Legislative Oversight." Legislative Studies Quarterly 9.3 (1984): 387-440. Print. 429.

good work in this field, since much of the information is sensitive and classified."[174] Rockman reached similar conclusions: "sustained and non-pluralistic oversight activity offers little payoff."[175] Senator Hubert Humphrey, excusing himself from a hearing on the CIA's involvement in Chile, presented the problem in a humorous, yet telling, statement: "I have to go now. I am trying to get jobs for 400 people in Minnesota today. That is a great deal more important to me than Chile."[176] Thus, with little political incentive to engage in intelligence oversight, Johnson asserts many in Congress realized it was politically safer to avoid responsibility for intelligence operations by simply looking the other way. As Senator Frank Church lamented, some in Congress held the position that "we don't know what's going on and, furthermore, we don't want to know."[177] These attitudes, David Colton explains in "Speaking Truth to Power: Intelligence Oversight in an Imperfect World," led to "an atmosphere in which accountability was the exception, and leniency the rule."[178]

All this is not to say that no members of Congress sought intelligence oversight reform during this period. But of the over 200 resolutions calling for improvements in oversight introduced in this period, "few managed to make it out of committee, and none was approved by Congress…only four represented serious initiatives."[179] The problem with these reform attempts, Johnson explains, is that "those persons seeking reform lacked the sine qua non for success: a sharply aroused public…As is frequently the case in the American political system, a truly major event was

---

[174] Johnson, Loch K. *A Season of Inquiry*. 8.
[175] Rockman, Bert. "Legislative-Executive Relations and Legislative Oversight." 429.
[176] Quoted in Colton, David: "Speaking Truth to Power." 583.
[177] Quoted in Johnson, Loch K. "Legislative Reform of Intelligence Policy." Polity 17.3 (1985): 549-573. Print. 551.
[178] Colton, David. "Speaking Truth to Power." 583.
[179] Johnson, Loch K. *A Season of Inquiry*. 8.

required to stir the public during demands for reform, in turn stimulating Congress to act."[180] Rockman corroborates this claim in his study, concluding, "crisis, publicity and corruption are strong external inducements to oversight. Such inducements provide opportunities for legislators to gain visibility at little cost."[181] Such an opportunity emerged on December 22, 1974, when the *New York Times* began to publish a series of articles by Seymour M. Hersh that "stirred a large number of citizens, aroused the national media, and prompted Congress to act."[182] And so ended the Era of Trust, as Congress turned public outcry into legislative action.

B. Oversight during the Era of Skepticism (1974-1976): A Rush to Reform

Hersh's series of articles accused the CIA of conducting "'massive' spying and illegal intelligence operations directed against antiwar activists and other American dissidents,"[183] compiling files of over 10,000 American citizens "in violation of the 1947 National Security Act that barred the CIA from any security or police function within the United States."[184] As an enraged public clamored for investigations into CIA's domestic spying, Congress quickly went to work responding with legislation. Even Senator Humphrey, who I quoted earlier downplaying the importance of oversight of intelligence activity, changed his tune. Ironically, Senator Humphrey called on members of Congress "to face up to a responsibility it has shirked for many years,"[185]–intelligence oversight. To that end, Senator Harold Hughes and Representative Leo Ryan proposed joint legislation

[180] Ibid. 9.
[181] Rockman, Bert. "Legislative-Executive Relations and Legislative Oversight." 429.
[182] Johnson, Loch K. "Legislative Reform of Intelligence Policy." 552.
[183] Johnson, Loch K. *A Season of Inquiry*. 9.
[184] Johnson, Loch K. "Legislative Reform of Intelligence Policy." 552.
[185] Johnson, Loch K. *A Season of Inquiry*. 10.

requiring the President to "approve and report to Congress about all important covert actions."[186] On December 30, 1974, just eight days after the publication of Hersh's report, President Gerald Ford signed the Hughes-Ryan Amendment into law.

In part, Congress' quick passage of the Hughes-Ryan Amendment was due to the fact that many of Congress' newest members campaigned aggressively against imperial presidency in the wake of the Watergate allegations; the Hughes-Ryan Amendment was their first chance to put rhetoric to action. Yet, perhaps reflecting how little time Congress had to debate pieces of legislation, the Hughes-Ryan provisions "quickly caused problems for both Congress and the Executive Branch."[187] Far from being a strong assertion of congressional power, Silverstein argues Congress inadvertently "provided for the first time some measure of explicit congressional authorization for covert action on the part of the executive and lent some legitimacy to executive claims to the autonomous power to covert action."[188] By requiring presidents to report to Congress about covert activity, Silverstein argues, "Congress implicitly sanctioned executive control of covert activities."[189] On January 27, 1975, the Senate voted overwhelmingly to establish a committee to conduct a nine-month investigation of American intelligence operations, leading Johnson to term 1975 the "Year of Intelligence."[190] Yet by the time the Church Committee formed to conduct these investigations and issue its findings, public support had turned against their investigation.

---

[186] Ibid. 10.
[187] McCormick, James, and Steven Smith. "The Iran Arms Sale and the Intelligence Oversight Act of 1980." 30.
[188] Silverstein, Gordon. *Imbalance of Powers*. 142.
[189] Ibid. 143.
[190] Johnson, Loch K. *A Season of Inquiry*. 11.

The purpose of the Church Committee's investigations into American intelligence operations, Johnson explains, was "to develop a new legislative charter for the intelligence community–to recast the National Security Act of 1947 so that it would more clearly define the limitations of and prohibitions on intelligence agencies."[191] But as the Church Committee in the Senate and the Pike Committee in the House of Representatives held hearing after hearing to determine what that those limitations on intelligence agencies would be, the investigations faced a public backlash. A poll conducted in December 1975 found that only 38 percent of Americans felt positively about the Church Committee, a finding Johnson deems "extremely disappointing…our long hours and careful research to uncover and guard against abuses by the intelligence services seemed to go largely unappreciated or misunderstood."[192] The source of the backlash is unclear, but Johnson cites the explanation by columnist Anthony Lewis, who argued that constituents disapproved of the "continuing exposure of secret operations. The members [of Congress] were hearing from back home that people were reluctant to hear about any more embarrassments on the American record."[193] Thus the Church Committee's findings were released when public support no longer backed sweeping reforms; when "many in Congress moved closer to accepting the argument that constitutional fidelity might have to give way to practical necessity when it came to foreign intelligence."[194] Even the Church Committee's conclusion that the Hughes-Ryan Amendment implicitly authorized covert action (as Silverstein argues) fell on apathetic ears–its recommendation that "Congress write full and explicit charters…to replace the outdated and vague National Security Act of 1947, never won legislative

[191] Johnson, Loch K. *A Season of Inquiry*. 227.
[192] Ibid. 185.
[193] Quoted in: *Ibid*. 185.
[194] Silverstein, Gordon. *Imbalance of Powers*. 143.

approval."[195] And so the investigations succeeded only in establishing two permanent intelligence oversight committees, one in each chamber of Congress. And as the "Year of Intelligence" wound to a close, with "the impetus for reform…only a shadow of what it was last year,"[196] reformers turned to make due with what support they had left.

C. Oversight during the Era of Uneasy Partnership (1977-1986): Fixing Hughes-Ryan

Acting accordingly with the decline in public support for intelligence oversight reform, Congress' goals in drafting the Intelligence Oversight Act of 1980 had a relatively modest goal: "to gain greater access to information within the executive branch regarding the conduct of intelligence policy. Put simply, an increasing number of legislators have wanted to know what was going on."[197] The 1980 Act required "prior notice to the intelligence committees, but it provided a few important loopholes,"[198] provisions I will discuss in the following section. Reformers seeking passage of the 1980 Act–or, as it was known in 1979, S Con Res 400–sought to make the legislation "appear as something so carefully worked out, so arduously labored over, and involving so many painful concessions by key senators that to question the results now would be an unthinkable faux pas."[199] To that end, in amendment after amendment, the 1980 Act was watered down in the Rules Committee, from decreasing the size of the Intelligence Committee to decreasing the committee's disclosure powers. Senator Abourezk criticized the concessions, saying he could "only presume that the drafters of the compromise

---

[195] Ibid. 143.
[196] Johnson, Loch K. *A Season of Inquiry*. 227.
[197] Ibid. 256.
[198] Silverstein, Gordon. *Imbalance of Powers*. 144.
[199] Johnson, Loch K. *A Season of Inquiry*. 233.

have more confidence in the judgment of the president than they do in the judgment of their own colleagues who will work on the new committee."[200]

Reflecting the fragility of the agreement, Senator Mansfield, the Democratic leader, said Abourezk's criticisms were "contrary to the compromise…which a lot of us worked awfully hard to achieve and to bring about the greatest degree of unanimity therein."[201] Unfazed, Abourezk shot back, asserting that the 1980 Act "compromises the power of the U.S. Senate to the president." Nonetheless, by a vote of 72-22, S Con Res 400 was passed into law as the Intelligence Oversight Act of 1980. In doing so, Congress strengthened its relationship with the CIA that had become strained over the last six years. As Stansfield Turner, who headed the CIA in 1980, explains, "once the committees had learned enough about intelligence to understand what we were doing and why, they were indeed willing to support us."[202] Despite the Rules Committee's amendments watering down the power of the Intelligence Oversight Committee, Johnson maintains that the "central recommendation of the Church committee had been adopted. The new fifteen-member committee had exclusive jurisdiction over the CIA…and it had the power of the subpoena to gather information from [intelligence] agencies."[203] Yet the compromises needed for the 1980 Act's passage ensured it would avoid "the tough constitutional questions of which branch had what powers in the intelligence field."[204] As the following section will show, shirking these questions had important constitutional implications.

---

[200] Ibid. 235.
[201] Ibid. 236.
[202] Turner, Stansfield S. *Secrecy and Democracy*. 150.
[203] Johnson, Loch K. *A Season of Inquiry*. 248.
[204] Silverstein, Gordon. *Imbalance of Powers*. 145.

In placing the 1980 Act in its historical context, I hope to make clear one very important point: that the atmosphere from which the 1980 Act emerged was far more hostile to sweeping reforms of intelligence oversight than during 1974-1976, and the language of the 1980 Act represented that reality. As Johnson admits, "the quest for the great charter failed."[205] Therefore, it is not fair to criticize the 1980 Act for failing to revolutionize intelligence oversight, given the environment in which it was passed. Yet the 1980 Act–"wrapped in ambiguous phraseology and consisting of only three pages"[206]– leaves much to critique, and it is to examining its "ambiguous phraseology" that I now turn.

Interpreting the Intelligence Oversight Act: A Textual Analysis

In research otherwise advocating autonomous Executive action in foreign affairs, Colton asserts "Congress' broad legislative power, combined with its power to declare war…give it ample justification to conduct extensive oversight of the Executive's intelligence activities."[207] Yet the text of the Intelligence Oversight Act of 1980 makes no mention of implicit Congressional constitutional authority, holding only that the provisions of the 1980 Act should be interpreted "to the extent consistent with all applicable authorities and duties, including those conferred by the Constitution upon the executive and legislative branches of Government."[208] In addition, the provisions of the 1980 Act are further qualified with the preface that it should be followed "with due regard for the protection from unauthorized disclosure of classified information and information relating to

---

[205] Johnson, Loch K. "Legislative Reform of Intelligence Policy." 556.
[206] Ibid. 556.
[207] Colton, David. "Speaking Truth to Power." 590.
[208] "Title 5, National Security Act of 1947 (50 U.S.C. 413 - Accountability for Intelligence Activities [Public Law 96-450])." [1980 Intelligence Oversight Act].(October 14, 1981): 1-9. Print. Sec. 501 (a).

intelligence sources and methods."[209] In this section, I explain why these two clauses, as well as multiple provisions of the 1980 Act, undercut Congress' oversight efforts by providing the Executive the explicit authorization to act alone.

A. Losing Legislative Leverage: Immediate Ambiguities

Despite the fact that the Constitution "does not overtly confer authority for intelligence activities to either the Congress or the President,"[210] Congress in the 1980 Act ceded its side of the constitutional debate without protest. The 1980 Act's first ambiguity, declining to define those "authorities and duties…conferred by the Constitution"[211] suggests an "effort of the Congress to avoid any explicit encroachment upon executive power."[212] Instead, Congress sought only to "enforce its right to receive information…merely for informational and consultative purposes [that] do not involve approval or permission."[213] Thus the 1980 Act "explicitly denied the intelligence committees authority to veto administration plans."[214] At best, the intelligence committees could only listen and be informed. By defining its own authority so narrowly, Congress avoided the hard-line attitude of the Pike Committee—who maintained "the bottom line is that the Congress has the right to receive classified information without any strings attached to it"[215]—relying instead "on the assumption that the Executive Branch would cooperate with Congress, and fulfill its half of the bargain."[216] Because, as Johnson asserts, "the

---

[209] Ibid. Sec. 501 (a).
[210] Colton, David. "Speaking Truth to Power." 587.
[211] *Intelligence Oversight Act of 1980*. Sec. 501 (a).
[212] Ibid *597.*
[213] Ibid. 597.
[214] McCormick, James, and Steven Smith. "The Iran Arms Sale and the Intelligence Oversight Act of 1980." 30.
[215] Johnson, Loch K. *A Season of Inquiry*. 79.
[216] Silverstein, Gordon. *Imbalance of Powers.* 146.

entire concept of a legislative check on the executive becomes a mockery without congressional information regarding Executive programs and plans,"[217] Congress left its oversight scope entirely in the hands of the Executive. As a House of Representatives study on intelligence oversight concluded, "All oversight is imperfect and is always limited by the degree to which the Executive Branch will be forthcoming with information."[218] Silverstein notes, this "acceptance of undefined instances when the President might withhold prior notice at his discretion gave congressional sanction to the Executive Branch's claim to prerogative powers."[219]

In addition, the clause covering "due regard for the protection from unauthorized disclosure of classified information"[220] perpetuates the false notion that Congress cannot be trusted with classified information; in fact, "Congress' record on keeping covert actions secret is excellent."[221] As Allan Goodman notes in an essay calling for intelligence reform, a Senate Select Committee on Intelligence study found that "only 14 of 150 [leaks studied] mentioned congressional aides as a source of information and that, of these stories, half cited administration sources as well."[222] In "Partisanship and the Decline of Intelligence Oversight," Marvin Ott takes this argument one step further: "Every serious assessment during the 1980s of the problem of 'leaks' of classified information into the public domain concluded that the sources were predominantly, if not overwhelmingly, in the

---

[217] Johnson, Loch K. *A Season of Inquiry*. 257.
[218] *IC21: the Intelligence Community in the 21St Century.* Print. Washington, DC: U.S. Government Printing Office, April 9, 1996. Print. Staff Study: Permanent Select Committee on Intelligence, House of Representatives, 104th Congress. 316.
[219] Silverstein, Gordon. *Imbalance of Powers.* 145.
[220] *Intelligence Oversight Act* of 1980. Sec. 501 (a).
[221] Goodman, Allan. "Reforming U. S. Intelligence." Foreign Policy 67 (1987): 121-136. Print. 132.
[222] Ibid. 132.

Executive Branch–including the Intelligence Community itself, not the oversight committees."[223] Turner concludes that he "found the congressional committees on intelligence as responsible as any sector of government, especially when it came to protecting our sources."[224] Nonetheless, the 1980 Act's assertion that its provisions only need be followed with due regard for preventing leaks of classified information provides the CIA and the President a loophole whereby they might withhold information from Congress for that very reason. Yet as I will demonstrate, these clauses are only *implicit* loopholes–the actual provisions of the 1980 Act provide *explicit* loopholes that undermine congressional oversight entirely, and grant unprecedented authority to an autonomous Executive.

B. The President and Prior Notice

In language better reflecting aggressive intelligence oversight, the 1980 Act requires all parties involved in intelligence activities to keep the congressional intelligence committees "currently informed of all intelligence activities…including any significant anticipated intelligence activity…"[225] By mandating prior notice of intelligence activities, this provision ostensibly makes sure Congress is kept in an active oversight role. Though the intelligence activities lack veto power, simply *knowing* what intelligence agencies (and the Executive to whom they answer) are doing puts them "in a position to advise–and perhaps to help avoid disasters like the Bay of Pigs and abuses like those uncovered by the *New York Times*."[226] As Goodman explains, "prior notification

---

[223] Ott, Marvin C. "Partisanship and the Decline of Intelligence Oversight." International Journal of Intelligence and Counterintelligence 16.1 (March 1, 2003): 69-94. Print. 78.
[224] Turner, Stansfield S. *Secrecy and Democracy*. 149.
[225] *Intelligence Oversight Act of 1980.* Sec 501. (a) (1).
[226] Johnson, Loch K. *A Season of Inquiry*. 256.

is not an unconstitutional infringement on the President's authority to conduct foreign relations. Notification is not a request for permission to act, but it probably would force administrations to think twice about resorting to risky paramilitary actions when congressional support is unlikely."[227] However, the prior notice provision, too, is undercut by an exception where, should the President determine it is "essential to limit prior notice to meet extraordinary circumstances affecting vital interests of the United States,"[228] he is required only to inform a group of eight congressional leaders.

However, even this provision provided room for the Executive to avoid congressional oversight–Lloyd Cutler, President Carter's legal adviser, recommended informing the intelligence committees immediately, "I have committed an action…[but] because of an extraordinary circumstance, a full reporting will have to be delayed."[229] Should the President decline prior notification of the intelligence committees, the 1980 Act mandates he "fully inform the intelligence committees in a timely fashion."[230] What is problematic about this provision is that the 1980 Act never defines the phrase "timely fashion," and, further complicating matters, McCormick and Smith note that "the committee reports and floor debates on the 1980 Act offer few useful clues as to Congress' interpretation"[231] of the phrase. William G. Miller, the former staff director of the Church committee, stressed that the "timely fashion" provision "was meant to apply only narrowly to the most exceptional cases."[232] Yet the problems this provision creates for Congress are clear: without

[227] Goodman, Allan. "Reforming U. S. Intelligence." 132.
[228] *Intelligence Oversight Act of 1980.* Sec 501. (a) (1) (B).
[229] Johnson, Loch K. *America's Secret Power*. 254.
[230] *Intelligence Oversight Act of 1980.* Sec 501. (b).
[231] McCormick, James, and Steven Smith. "The Iran Arms Sale and the Intelligence Oversight Act of 1980." 34.
[232] Johnson, Loch K. *America's Secret Power*. 253.

clearly defining "timely," the President is free to define it himself. Thus "when the President asserts constitutional authority to forego prior notice he may use the same authority to delay reporting indefinitely, defining 'timely' in terms of the needs of the executive branch rather than the needs of Congress."[233] This provision, therefore, represents "a direct challenge to congressional oversight."[234]

In light of this reporting loophole, McCormick and Smith posit that the 1980 Act actually "diffused responsibility and obscured the President's personal responsibility to report to Congress."[235] Because the 1980 Act did not address explicitly situations where the President supervises intelligence activities, the President's reporting responsibilities remained unclear. The 1980 Act only charges the President with reporting to Congress when the intelligence agencies decline to give Congress prior notice of intelligence activity. Thus so long as the intelligence agencies continue to do so, the President himself may decline to report to Congress himself, presenting another example where the 1980 Act diminished Congress' check on the Executive Branch.

By picking apart problematic language in the Intelligence Oversight Act of 1980, I sought to provide textual support for Silverstein's assertion that the 1980 Act "provided statutory requirement for reporting, but in so doing…it provided legislative authorization for conducting [intelligence] activities, under certain specified conditions, without informing Congress in advance."[236] As McCormick and Smith argue, "the only defense for such a sweeping avoidance of notification requirements can be a

---

[233] McCormick, James, and Steven Smith. "The Iran Arms Sale and the Intelligence Oversight Act of 1980." 34.
[234] Currie, James T. "Iran-Contra and Congressional Oversight of the CIA."
[235] McCormick, James, and Steven Smith. "The Iran Arms Sale and the Intelligence Oversight Act of 1980." 33.
[236] Silverstein, Gordon. *Imbalance of Powers*. 145.

constitutional one…inherent in [the President's] commander-in-chief authority. If this is a valid defense, it undermines both prior notice and timely fashion requirements of the Act, contrary to Congress' hope."[237] Even Turner declares it "Congress' job to judge how well the president has used his authority in the past, and, if necessary, to enact legislation that enlarges or limits that authority. This distinction is central to the constitutional balance of powers."[238] Viewed from that perspective, Silverstein's original conclusion is corroborated by the text of the 1980 Act–by granting the President power to act with neither prior notice nor congressional oversight, Congress effectively gave "sanction to the Executive Branch's claim to prerogative powers."[239] Johnson noted in 1985 that the Intelligence Oversight Act of 1980's "ambiguities and shortfalls will haunt overseers of serious intent."[240] In the following section, I look to the Iran-Contra affair to show how Reagan utilized these ambiguities and shortfalls to bypass congressional oversight altogether.

Intelligence Oversight during Iran-Contra and Beyond

In April 1984, CIA Director William Casey was accused of failing to properly inform Congress of CIA involvement in the mining of Nicaraguan harbors. As a result, Casey "agreed, in writing, to provide prior notice to the Senate Intelligence Committee of all significant covert operations."[241] Yet on January 17, 1986, after approving the shipment of arms to Iran, President Reagan "ordered Casey not to provide prior notice to the

[237] McCormick, James, and Steven Smith. "The Iran Arms Sale and the Intelligence Oversight Act of 1980." 34.
[238] Turner, Stansfield S. *Secrecy and Democracy*. 130.
[239] Silverstein, Gordon. *Imbalance of Powers.* 145.
[240] Johnson, Loch K. "Legislative Reform of Intelligence Policy." 569.
[241] McCormick, James, and Steven Smith. "The Iran Arms Sale and the Intelligence Oversight Act of 1980." 31.

intelligence committees of Congress,"[242] violating the 1980 Act's insistence that such agencies keep Congress "fully and currently informed of all intelligence activities."[243] Using the Iran-Contra affair as an example, I will demonstrate how Congress' "reluctance to engage the executive in constitutional debate…undermined the objectives Congress set for the reform legislation."[244]

A. Undermining Oversight in the Iran-Contra Affair

Through textual analysis, I demonstrated how the loopholes written into the 1980 Act provided statutory justification for President Reagan's order that Casey withhold this information. Yet in so doing, President Reagan undercut the entire tradeoff Congress had hoped to make: ceding constitutional authority and approval to the Executive, in exchange for the Executive keeping Congress informed of intelligence activities. As James Currie notes his report on "Iran-Contra and Congressional Oversight of the CIA," by hiding the Iranian arms transfer, "President Regan forfeited the benefit of advice from senior elected officials of the government–men and women who might have dissuaded him from undertaking an effort that tarnished the success of his administration…congressional opposition to the Iranian covert action might have prevented one of the most damaging and embarrassing episodes in recent American foreign policy."[245] Those hoping the 1980 Act would lead to consistent consultation with Congress had to be concerned by a statement made by Reagan's press secretary, Larry Speakes, who argued that the

---

[242] Ibid. 31.
[243] *Intelligence Oversight Act of 1980.* Sec 501. (a) (1).
[244] Silverstein, Gordon. *Imbalance of Powers.* 168.
[245] Currie, James T. "Iran-Contra and Congressional Oversight of the CIA." 203.

"judgment was made that it [reporting to Congress] was not necessary under the law."[246]

As Turner argues, the Reagan administration's "willingness repeatedly to flout the Congress reflected a view that oversight as an impediment rather than a necessity for good intelligence in a society like ours."[247] The release of a memo written by Lt. Col. Oliver North advising President Reagan affirmed concerns that the ambiguities in the 1980 Act would be interpreted to grant incredible leeway to the Executive. In the memo, Lt. Col. North recommends that President Reagan exercise his "statutory prerogative to withhold notification of the finding to the congressional oversight committees until such time that you deem it to be appropriate."[248] The wording here is of the utmost importance–Lt. Col. North asserted *statutory* prerogative written into the 1980 Act, instead of advising President Reagan to rely on implicit constitutional authority. Here we have clear evidence that supports the claim I sought to evaluate in this paper: that the 1980 Act "provided fresh and unprecedented explicit authorization for executive prerogative."[249] Consequently, the 1980 Act has far-reaching implications on the Constitution's separation of powers, inasmuch as this statutory acceptance of the executive prerogative "added to the growing *constitutional* case for the prerogative interpretation."[250]

In sum, the historical record of the Iran-Contra affair suggests that the ambiguities and loopholes written into the 1980 Act were both recognized and utilized by the Executive Branch to avoid consultation with Congress, and as a result undercut

---

[246] Quoted in: McCormick, James, and Steven Smith. "The Iran Arms Sale and the Intelligence Oversight Act of 1980." 34.
[247] Turner, Stansfield S. *Secrecy and Democracy*. 172.
[248] McCormick, James, and Steven Smith. "The Iran Arms Sale and the Intelligence Oversight Act of 1980." 31.
[249] Silverstein, Gordon. *Imbalance of Powers*. 145.
[250] Ibid. 145.

intelligence oversight altogether. As McCormick and Smith write, the "central purpose of the [1980 Act], to provide a mechanism for consultation with Congress, was deliberately undermined."[251] The efforts reforming congressional oversight of intelligence activities during the 1970s reflected Turner's assertion that, overall, "congressional oversight strengthens intelligence capabilities."[252] That the 1980 Act provided constitutional justification for eschewing intelligence oversight and strengthened the Executive's constitutional claim to an unchecked prerogative power constitutional certainly undercuts Johnson's assertion that the 1980 Act "catches much of the spirit, and at least some of the substance, that sustained reformers during the Year of Intelligence."[253] An informed Congress could have advised the Reagan Administration against participating in the Iran-Contra exchanges, or could have cut funding for these intelligence activities. But in writing the 1980 Act, Congress gave the President statutory justification to ignore them altogether. However, it would be unfair to give no voice to Johnson and others who defend the 1980 Act, despite its failure to constrain the Executive in the Iran-Contra affair.

B. Defending the 1980 Act in Light of the Iran-Contra Revelations

I want to highlight some of the defenses of the 1980 Act because I do believe it is unfair to criticize the 1980 Act's every imperfection as if it were written by constitutional scholars, and not by political actors operating in a dynamic legislative environment. By placing the 1980 Act in historical context, I hoped to highlight the difficulties and compromises necessary for the 1980 Act's passage, especially given the steep decline in public

---

[251] McCormick, James, and Steven Smith. "The Iran Arms Sale and the Intelligence Oversight Act of 1980." 34.
[252] Turner, Stansfield S. *Secrecy and Democracy*. 130.
[253] Johnson, Loch K. "Legislative Reform of Intelligence Policy." 569.

support for intelligence oversight reform. Criticisms of the ambiguities written into the 1980 Act must be qualified by the realities of the political process–as Johnson both recognizes these flaws but maintains they represented "the price of passage in 1980."[254] As Turner points out, a danger of congressional oversight "comes from the impulse of congressional committees to manage rather than just oversee."[255] In this respect, Johnson argues, we must recognize that as "legislative proposals become very specific they tend to lose support in Congress as the glue of ambiguity vanishes and the Executive, fearful of losing leeway, redoubles its opposition."[256] Because in 1980 the "broad consensus for charter reform no longer existed,"[257] perhaps scholars should be content with the fact that 1980 Act "reversed the reigning assumption about oversight,"[258] putting the burden of informing Congress on the Executive Branch. For this reason, Johnson argues, an Executive avoiding congressional oversight on a given intelligence operation risks losing a great degree of political capital if the operation fails, taking the whole of the blame.[259]

Another criticism of my analysis might argue that I should "avoid drawing general conclusions from exceptional, even if important, cases" [260] like the Iran-Contra scandal. As Colton notes, "outside the Iran-Contra incident, the compromise system embedded in the 1980 Oversight Act has worked fairly well. It should be strengthened, not discarded."[261] Johnson asserts that that "while this proved to be untrue for the Iran-contra operation, intelligence policy for the most part did become more of a

---

[254] Ibid. 569.
[255] Turner, Stansfield S. *Secrecy and Democracy*. 130.
[256] Johnson, Loch K. "Legislative Reform of Intelligence Policy." 572.
[257] Silverstein, Gordon. *Imbalance of Powers*. 144.
[258] Ibid. 145.
[259] Johnson, Loch K. "Legislative Reform of Intelligence Policy." 561.
[260] Johnson, Loch K. *America's Secret Power*. 248.
[261] Colton, David: "Speaking Truth to Power." 613.

partnership between the branches than ever before."[262] What is problematic about arguing the Iran-Contra affair as an exception is that it ignores the fact that congressional oversight is *most* important on these so-called "exceptional" circumstances, at least insofar as Congress hoped to avoid repeating intelligence failures such as the Bay of Pigs. Such an intelligence failure occurred on September 11, 2001. In their report released in 2004, the 9/11 Commission "concluded that congressional oversight of intelligence was 'dysfunctional.'"[263] Despite congressional efforts again to reform intelligence oversight in 1991, Congress's failure to address questions of explicit constitutional powers undercut any attempt to reassert any constitutional right to be informed of intelligence activities. The 1980 Act may indeed have increased the role of Congress "in terms of day-to-day oversight and administration of the intelligence community,"[264] but any fair assessment of the 1980 Act must weigh those gains against potential losses of constitutional authority, ceded to the Executive Branch. In the conclusion, I turn to assess that very tradeoff.

Concluding Thoughts: The 1980 Act in a Current Context

In this paper I investigated in depth the Intelligence Oversight Act of 1980, in order to assess Silverstein's conclusion that with this act, "Congress' attempt to control the executive's actions in foreign policy only provided fresh and unprecedented explicit authorization for executive prerogative."[265] I argued that this was a multi-step process. Seymour Hersh's series of articles set Congress off into aggressive investigation of intelligence

---

[262] Johnson, Loch K. *America's Secret Power*. 249.
[263]Kaiser, Frederick M. *Congressional Oversight of Intelligence: Current Structure and Alternatives.* Washington, DC: Congressional Research Service. September 16, 2008. Print. CRS Report for Congress. 5.
[264] Silverstein, Gordon. *Imbalance of Powers.* 145.
[265] Ibid. 145.

agencies; as time passed, public support for intelligence oversight reform declined. As a result, some of the core reform recommendations were passed over in favor of compromise legislation riddled with ambiguities and problematic provisions and concessions. These in turn provided the Executive with statutory and constitutional authorization to ignore oversight and undermine Congress' role in overseeing intelligence. Thus I concur with Silverstein's conclusion, providing both historical and textual evidence to explain why.

Power struggles between the various branches of government are built into the American system of government to ensure each branch provides checks and balances on the other. While the 1980 Act represented a setback for Congress in checking Executive authority in intelligence activities, we can view the 1980 Act as but another part of Congress' historical vacillation "between benign neglect of its oversight power and zealous overreaching,"[266] with no end in sight. I think it is important to recall the words of Justice Potter Stewart, who famously declared, "the Constitution…establishes the contest, not its resolution."[267] I do not know the perfect prescription for balancing Congress and the Executive in conducting intelligence activity; moreover, I am unconvinced that there is such a solution. As Johnson admits, "we seem to lack the knowledge–certainly we lack a theory of intelligence–to draft laws so well balanced as to prevent abuses while allowing executive flexibility to meet unforeseen contingencies."[268]

However, what we do know is that the Intelligence Oversight Act of 1980, while seemingly increasing Congress'

---

[266] Colton, David: "Speaking Truth to Power." 582.
[267] Stewart, Potter. 1975 speech to Yale Law School, Quoted in: Overholser, Geneva, and Kathleen Hall Jamieson. The Press. USA: Oxford University Press, 2006. Print. 269.
[268] Johnson, Loch K. "Legislative Reform of Intelligence Policy." 572.

influence in monitoring intelligence activity, contained provisions that helped to support the executive prerogative interpretation, thereby allowing the Executive Branch to violate the Constitution's separation of powers by acting unchecked by congressional oversight. The tragedy of the September 11, 2001 attacks, followed by the 9/11 Commission's conclusion that the congressional oversight of intelligence was "dysfunctional," should make us strive to improve intelligence oversight. However, the House of Representatives and the Senate declined to follow the 9/11 Commission's recommendation of creating a Joint Committee on Intelligence that might more successfully constrain Executive action and reverse the "ever-lengthening history of congressional deference to the executive."[269] Twenty-four years have passed since the enactment of the 1980 Act, and Congress still struggles to enact effective oversight over intelligence activity. As Senator Mathias puts it, "the courage that matters is the courage to stand alone and blow the whistle day by day."[270] By clearly defining their constitutional authority to act in intelligence-related legislation, Congress can learn from their mistakes in the 1980 Act and "blow the whistle" on unconstitutional Executive action, thereby reaffirming the core goal of the reform movement in the 1970s: intelligent oversight.

[269] Silverstein, Gordon. *Imbalance of Powers*. 147.
[270] Johnson, Loch K. *A Season of Inquiry*. 276.

Works Cited

Colton, David. "Speaking Truth to Power: Intelligence Oversight in An Imperfect World." *University of Pennsylvania Law Review* 137.2 (1988): 571-613. Print.

Currie, James T. "Iran-Contra and Congressional Oversight of the CIA." *International Journal of Intelligence and Counterintelligence* 11.2 (June 1, 1996): 185-210. Print.

Goodman, Allan. "Reforming U. S. Intelligence." *Foreign Policy* 67 (1987): 121-136. Print.

IC21: the Intelligence Community in the 21St Century. Print. Washington, DC: U.S. Government Printing Office, April 9, 1996. Print. Staff Study: Permanent Select Committee on Intelligence, House of Representatives, 104th Congress.

Johnson, Loch K. *America's Secret Power: the CIA in a Democratic Society*. New York, NY: Oxford University Press, 1989. Print.

---. "Legislative Reform of Intelligence Policy." *Polity* 17.3 (1985): 549-573. Print.

---. *A Season of Inquiry: the Senate Intelligence Investigation*. Lexington, KY: The University Press of Kentucky, 1985. Print.

Kaiser, Frederick M. *Congressional Oversight of Intelligence: Current Structure and Alternatives*. Washington, DC: Congressional Research Service, Library of Congress, September 16, 2008. Print. CRS Report for Congress.

McCormick, James, and Steven Smith. "The Iran Arms Sale and the Intelligence Oversight Act of 1980." *PS* 20.1 (1987): 29-37. Print.

Ott, Marvin C. "Partisanship and the Decline of Intelligence Oversight." *International Journal of Intelligence and Counterintelligence* 16.1 (March 1, 2003): 69-94. Print.

Overholser, Geneva, and Kathleen Hall Jamieson. *The Press*. USA: Oxford University Press, 2006. Print.

Rockman, Bert. "Legislative-Executive Relations and Legislative Oversight." *Legislative Studies Quarterly* 9.3 (1984): 387-440. Print.

Silverstein, Gordon. *Imbalance of Powers: Constitutional Interpretation and the Making of American Foreign Policy*. New York : Oxford University Press, 1997. Print.

"Title 5, National Security Act of 1947 (50 U.S.C. 413 - Accountability for Intelligence Activities [Public Law 96-450])." [1980 Intelligence Oversight Act].(October 14, 1981): 1-9. Print.

Turner, Stansfield S. *Secrecy and Democracy: the CIA in Transition*. New York, NY: Perennial Library, 1986. Print.

Cocaine:
Federal Sentencing Policy and its Implications on the Urban Community

By: Taniel Baghdikian

Introduction

Throughout history nations have implemented policies and participated in events that today would be considered regrettable. The United States has been no stranger to these. The internment of the Japanese, segregation, the Vietnam War, and, most recently, the Iraq War were all thought to be in the best interest of the country, but ended up being human rights violations and political blunders that had negative implications for society. Over the last decade, this nation's politicians, lawmakers, and human rights activists have begun to take a closer look at the laws governing criminal sentencing for the use and trafficking of cocaine. More specifically, they've contested the discrepancy between two different pharmacological compositions of cocaine: cocaine hydrochloride (powder) and cocaine base (crack). This paper's main objective is to address and determine the extent of the disparity in sentencing policy between powder and crack cocaine, why this disparity exists, and the effect it has on different races, ethnicities, and communities.

To best explain the main objective, the paper will survey:

- the chemical composition of powder and crack cocaine and their respective physiological and psychoactive effects,
- analyze statistics to determine if certain types of cocaine attract specific demographics,
- analyze the sentencing laws and mechanisms used to create and modify the policies,
- recall instances of the drug in the media and the attention that it drew to the issue,
- and list people, groups, and organizations that affect or are affected by the policies in place.

Pharmacology

Society has a commonly held belief that the chemical composition differences in crack cocaine, compared to powder

cocaine, produce more violent, addictive, and harmful behavior from its users. However, neuroscientists from the University of Minnesota and a panel of physical, social, and medical scientists testifying in front of the United States Sentencing Commission (USSC) insist that the commonly held belief is no more than an urban legend or myth and that the true differentiation between powder and crack cocaine is in its administration.[271]

Powder cocaine comes in a hydrochloride salt form. From this, it is mixed with baking soda and boiled in order to form a neutralized compound, referred to as free-base, or more commonly, crack. Powder and crack have a similar chemical make-up. Therefore, the difference lies in the method of intake. Powder cocaine can be administered intranasaly, orally, or intravenously. Crack is almost always smoked. Intravenous injection and smoking are the fastest-acting and most potent ways to administer cocaine.[272] It is, however, "much easier to smoke a drug than to inject it" in order to reach the quick and potent high that most users look for, according to Dr. Nora D. Volkow.[273]

Cocaine has effects on the central nervous, cardiovascular, and digestive system. These effects include euphoria, energy, alertness, loss of appetite, and sleep loss.[274] The intake of high concentrations of cocaine, which is easily accomplished when the drug is taken intravenously or by smoking, can lead to violent paranoia and bizarre psychotic behavior.[275]

---

[271] Federal Sentencing Reporter, Vol 14. No. 3-4. 2001-2002. US Sentencing Commission Hearing 2/25/02: Cocaine Pharmacology, Crack Babies, Violence. 191-196

[272] Ibid.

[273] United States Sentencing Commission Report to the Congress: Cocaine and Federal Sentencing Policy. May 2002. 63.

[274] Federal Sentencing Reporter, Vol 14. No. 3-4. 2001-2002. US Sentencing Commission Hearing 2/25/02: Cocaine Pharmacology, Crack Babies, Violence.

[275] Ibid.

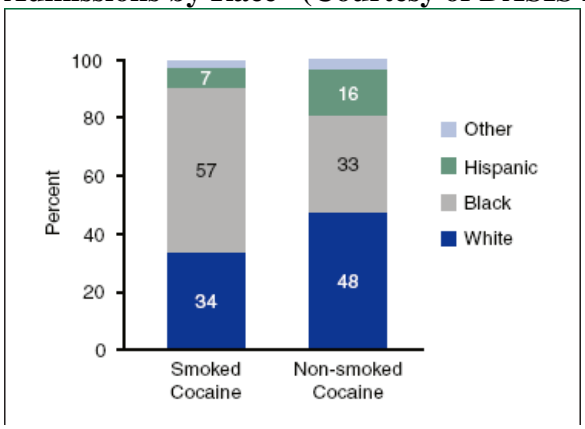
Demographics of Use

Race, Ethnicity, National Origin

There are two key sources of data used to determine the demographic characteristics of cocaine users. 1) The United States Sentencing Commission's record of arrests for powder and crack cocaine offenders (includes manufacturing, trafficking, and dealing offenses). 2) And, the Drug and Alcohol Information System (DASIS) report's data collected from the Treatment Episode Data Set (TEDS) of admissions to rehabilitation centers and hospitals.

By comparing these two sets of data, one can conclude that the majority of crack cocaine use is by blacks. Yet in the case of powder cocaine, the majority of those arrested are Hispanic, and the majority of those admitted to rehabilitation are white [See Appendix – A1 "Demographic Characteristics of Federal Cocaine Offenders" and Figure 1, below].[276]

Figure 1. "Smoked and Non-Smoked Cocaine Admissions by Race" (Courtesy of DASIS Report)[277]

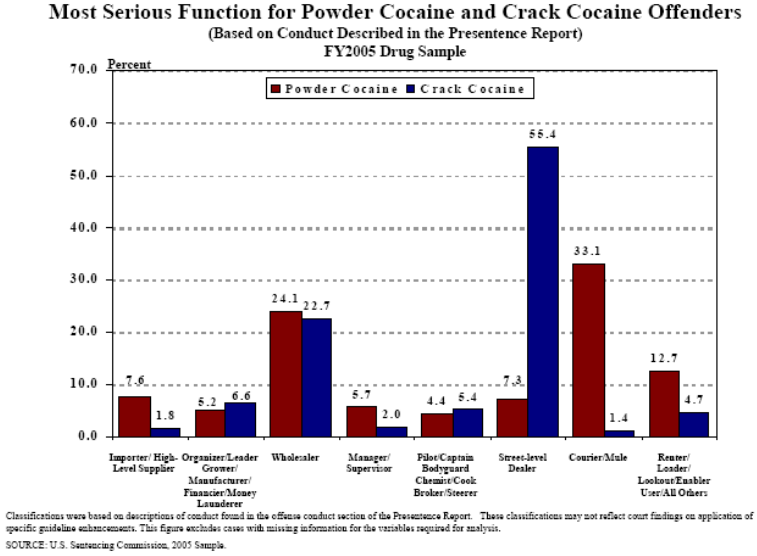


[276] United States Sentencing Commission Report to the Congress: Cocaine and Federal Sentencing Policy. May 2007. 16.

[277] Drug and Alcohol Services Information System. "The DASIS Report". February 25, 2005. 2.

The information in the Appendix A-1 and Figure 1 may seem conflicting. However, the majority of the U.S. cocaine supply is imported from South America and Mexico. It is delivered to the U.S. by couriers, often referred to as "mules," who are almost always Hispanic. Almost all crack cocaine is manufactured and trafficked domestically. As the data in Figure 2 ("Most Serious Function for Powder Cocaine and Crack Cocaine Offenders") shows, the majority of powder cocaine arrests are of couriers, while the majority of crack cocaine offenses are by street-level dealers.[278] Therefore, the information from the DASIS report would lead one to assume that the majority of powder cocaine *users* are white.

Figure 2 – (Courtesy: USSC)



[278] United States Sentencing Commission Report to the Congress: Cocaine and Federal Sentencing Policy. May 2007. 18-19.

Price

Prices for powder and crack cocaine are estimated from the United States Drug Enforcement Administration's (DEA's) System to Retrieve Information from Drug Evidence (STRIDE) database. Their data concludes that, on average, the price of powder and crack cocaine is similar at each quantity point.[279] This data is contrary to popular belief today and the "expert" belief in the 1980s that the "cheap" nature of crack was responsible for its rapid spread through the ghettos of the United States. This misconception was a contributing factor to the harsher sentencing policies enacted concerning crack cocaine with the passing of the Anti-Drug Abuse Act of 1986.[280]

It should be noted that although price per unit is similar between powder and crack cocaine, crack has a reputation of being sold in smaller quantities than powder cocaine.[281]

Laws and Policies

Anti-Drug Abuse Act of 1986

The Anti-Drug Abuse Act of 1986 established mandatory minimum penalties for cocaine and various other drugs. The Act differentiated between crack and powder cocaine because, at the time, it was perceived that crack was highly addictive, induced violent crime, its physiological effects often resulted in death, it was low cost, and it was relatively easy to manufacture, transport, and administer. (Correlation between crack cocaine and crime will

---

[279] United States Sentencing Commission Report to the Congress: Cocaine and Federal Sentencing Policy. May 2007. 90-94.
[280] United States Sentencing Commission Report to the Congress: Cocaine and Federal Sentencing Policy. May 2002. v-vii.
[281] Fryer, Roland. National Bureau of Economic Research. Measuring the Impact of Crack Cocaine. May 2005. 4.

be discussed in the "Impact on Urban Community" section of this paper.)

The 1986 Act specifically established what has come to be known as the "100:1 ratio". This ratio refers to the disparity in quantity between powder cocaine and crack cocaine that triggers the mandatory minimum sentencing penalty. Specifically, a five year minimum mandatory jail sentence is required for anyone trafficking 500 grams of powder cocaine, or 5 grams of crack cocaine. In other words, it takes 100 times more powder cocaine to receive the same minimum mandatory sentence as crack cocaine.[282]

In order to determine sentencing, courts use a schedule of Base Offense Levels. Each range of quantities for cocaine has a respective Base Offense Level. Each level corresponds to a different sentence length. Criminal history is also taken into consideration when determining sentence length. See Appendix A-2, "2003 Federal Sentencing Guidelines."[283] The "100:1" ratio applied to this schedule until the November 1, 2007 USSC Amendment was ratified (See "USSC Amendment" section of this paper).

The U.S. Sentencing Commission, in its report to Congress in 2002, states that, "When Congress passed the 1986 Act, the Commission had not completed promulgating the initial sentencing guidelines [that it deemed appropriate]."[284] The USSC's guidelines recommended different sentencing guidelines than those set forth by the 1986 Act concerning crack cocaine, yet it cites an expedited passing of the 1986 Act as the reason for its incomplete notice of

---

[282] United States Sentencing Commission. Report to the Congress: Cocaine and Federal Sentencing Policy. May 2002. 4-13.
[283] United States Sentencing Commission. An Overview of the Federal Sentencing Guidelines. 3. <http://www.ussc.gov/2003guid/tabcon03.htm>
[284] United States Sentencing Commission Report to the Congress: Cocaine and Federal Sentencing Policy. May 2002. iv-v.

its own initial guidelines. For this reason, the U.S. Sentencing Commission incorporated the guidelines set forth by the 1986 Act.

Congress's reason for expediting the usual legislative process in order to pass the 1986 Act is that there was a national sense of urgency caused by heightened media attention resulting from the death of public icons, such as the 1986 NBA number two draft pick, Len Bias, who overdosed on cocaine 48 hours after being selected by the Boston Celtics.[285]

The Omnibus Anti-Drug Abuse Act of 1988 extended the same penalties for crack cocaine trafficking to people arrested for simple possession of five grams.[286] This was another example of harsher penalties for crack possession than its equivalent in powder form and a contributing factor to the sentencing disparity between crack and powder users.

USSC Amendment

On May 1, 2007, the USSC submitted its most recent Federal cocaine sentencing guidelines report. In the report, it recommended that Congress lower sentencing ranges for Base Offense Levels associated with crack cocaine quantities. The amendment became effective on November 1, 2007.[287] It lowered the Base Offense Level of every range of crack cocaine from 250mg to 4.5kg by two levels. Although sentencing guidelines for powder and crack cocaine are not equal, as a direct result of the amendment, the 100:1 disparity ratio no longer exists.[288] See Figures 3 & 4.

---

[285] Ibid, v.
[286] Ibid.
[287] National Public Radio Website. Nov 2, 2007. US Sentencing Ranges Lowered for Crack Cocaine. Nov 30, 2008.
[288] Sentencing Resource Counsel. Nov 1, 2007. "Applying the Crack Amendments 101." 1-2.

Figure 3 – Old and New Base Offense Level Chart. (Courtesy: Sentencing Resource Counsel)[289]

Quantity	BOL under Former § 2D1.1	BOL under Amended § 2D1.1
4.5 KG or more	38	38
1.5 KG to < 4.5 KG	38	36
500 G to < 1.5 KG	36	34
150 G to < 500 G	34	32
50 G 50 < 150 G	32	30
35 G to < 50 G	30	28
20 G 50 < 35 G	28	26
5 G to < 20 G	26	24
4 G to < 5 G	24	22
3 G to < 4 G	22	20
2 G to < 3 G	20	18
1 G to < 2 G	18	16
500 MG to < 1 G	16	14
250 MG to < 500 MG	14	12
< 250 MG	12	12

[289] Ibid.

Figure 4 – New Powder to Crack Cocaine Ratio. (Courtesy: Sentencing Resource Counsel)[290]

LEVEL	RATIO
38	33:1
36	33:1
34	30:1
32	33:1
30	70:1
28	57:1
26	25:1
24	80:1
22	75:1
20	67:1
Lower	50:1

This amendment applies retroactively to prisoners currently serving sentences for crack cocaine trafficking and/or possession.

Case Law

United States v. Booker

The 2005 ruling in *United States v. Booker* paved the way for the decision in *Kimbrough v. United States*. The U.S. Supreme Court held that the Federal sentencing guidelines are advisory, and can be deviated from if the sentence of a defendant exceeded the high end of the range specified in USSC's sentencing table.[291]

Kimbrough v. United States

The ruling in the court case of *Kimbrough v. United States* is regarded as one of the most important judgments in sentencing

[290] Sentencing Resource Counsel. Nov 1, 2007. "Applying the Crack Amendments 101." 1-2.
[291] United States Sentencing Commission. Final Report on United States v. Booker On Federal Sentencing. March 2006. 1-10.

policy for crack cocaine. On December 10, 2007, the U.S. Supreme court ruled that the sentence given to Kimbrough, if calculated using the current crack cocaine guidelines, would have been "disproportionate and unjust… greater than necessary to accomplish the purposes set forth."[292] This ruling set the precedent that federal judges have the discretion to shorten sentencing terms for crack cocaine offenses in instances when sentencing guidelines call for a punishment that is "greater than necessary."[293]

Advocates & Opposition

Advocates

The United States Sentencing Commission

On May 1, 1995, the USSC submitted to Congress an amendment to the 1986 and 1988 Acts setting forth an equalization of guideline penalties for powder and crack cocaine offenses based solely on quantity. The amendment also called for harsher penalties for powder and crack offenses that involved the use of weapons and/or violence.[294] (The fate of this amendment is discussed in the "Opposition" section of this paper). In addition to the proposed amendment, the USSC includes in every report to Congress regarding Federal cocaine sentencing policy a recommendation that the sentencing guidelines for powder and crack be reconsidered. On May 1, 2007, the USSC submitted to Congress yet another amendment to the 1986 and 1988 Acts. This time however, instead of completely leveling the disparity between powder and crack cocaine, it reduced it [See "Laws and Policies" section for details]. To date, Congress has not challenged this amendment and it went into effect on November 1, 2007.

---

[292] Supreme Court of the United States. Slip Opinion, Syllabus. October Term 2007. December 10, 2007. Kimbrough v. United States. Dec 5, 2008. 1-6.
[293] Ibid.
[294] United States Sentencing Commission Report to the Congress: Cocaine and Federal Sentencing Policy. May 2002. v.

Groups, Organizations, and Lobbies

The American Bar Association (ABA), American Civil Liberties Union (ACLU), Families Against Mandatory Minimums (FAMM), and the Sentencing Project are all existing groups that advocate an abolishment of the sentencing disparity between powder and crack cocaine. Unlike the other groups, Crack the Disparity's only issue is the Federal crack cocaine sentencing disparity. Yet, it's goal is similar to those of the other organizations: to promote equality within the U.S. justice system.

Opposition

104th United States Congress & President Bill Clinton

The 104th United States Congress passed legislation disapproving the USSC's May 1, 1995 amendment to equalize sentencing guidelines immediately after it was introduced. Congress's bill was then signed by President Bill Clinton.[295] However, it is important to note that the 110th Congress has not challenged the amendment submitted to them on May 1, 2007 and ratified on November 1, 2007.

U.S. Attorney General & the Department of Justice

U.S. Attorney General and the Department of Justice have held a long-standing position that the sentencing laws and policies, prior to the amendment by the USSC, were reasonable.[296]

The Attorney General of President George W. Bush's Administration, Michael Mukasey, was strongly opposed to and testified against the amendment that eventually became effective on November 1, 2007.[297] He claims that the easing of sentencing

---

[295] Ibid,12.

[296] USSC. Public Hearing on Cocaine Sentencing Policy. November 14, 2006. 12.

[297] Watts, J.C., Washington Times. Feb 12, 2008. "Reforming Crack Cocaine Law". <http://www.washingtontimes.com/news/2008/feb/12/reforming-crack-cocaine-law/> Nov. 29, 08.

guidelines would flood the streets with criminals that could potentially terrorize communities.[298]

Impact on Urban Community

Crack cocaine is mostly found in urban communities. Although not all of the data presented in this paper exclusively represents the urban community, the amount of data representing areas other than urban, in regards to crack cocaine, is relatively insignificant. Therefore, the data sets concerning crack cocaine arrests, admissions to rehabilitation/hospitals, violence, crime, etc. are assumed to be representations of the urban community.

The Black Community

The black community is greatly affected by the crack cocaine epidemic and its associated risks and implications. According to Professor Malo Hutson of UC Berkeley, "The 100 largest metropolitan areas are now a majority of non-white or Latino."[299] There is a correlation of crack use between the black community and the urban community. However, there is no indicator of causation. In other words, there are no credible studies that identify a cause of the correlation. It is unclear if crack is an epidemic of the black community that is correlated to the urban community due to the high percentage of blacks that populate urban communities or whether crack cocaine is an epidemic of the urban community that correlates to the black community.

However, after reviewing data in Appendix A-1, described in the "Demographics of Use" section of this paper, one can see that Hispanic use of crack cocaine is minimal, making up less than

---

298 Frieden, Terry. "Mukasey Wants Police Support to Prevent Prisoner Releases". Feb 26, 2008, CNN.com. <http://www.cnn.com/2008/CRIME/02/25/cocaine.sentencing/> Dec 1, 2008.

299 Professor Malo Hutson. Lecture on Oct 8, 2008. "Race and Ethnic Relations, Part 2". UC Berkeley.

9% of the offenses compared to almost 82% by blacks.[300] This data invokes the question, "How has the Hispanic community, while also living in urban areas, avoided infection by the crack cocaine epidemic?" Professor Malo Hutson states that there is a trend in black neighborhoods to remain segregated and not to racially integrate with whites, Asians, or Hispanics. So, although cities in the United States are becoming more and more racially diverse, black neighborhoods are not.[301] Therefore, the quarantining of the crack cocaine epidemic to black neighborhoods is a possible reason for the disproportionately high percentage of black crack users.

Allegations of Institutional Racism

Due to this disproportionate usage demographic of crack cocaine by blacks, organizations and individuals, including UC Berkeley Law Professor, David Sklansky, have made allegations of institutional racism by U.S. legislators.[302] Of course, it is unclear if it was the intent of law makers to persecute the black community by enacting the crack cocaine sentencing laws. However, it is clear that those laws do in fact pose disproportionate burden on the black community.

Crime and Violence

Several studies have been conducted in order to determine crack cocaine's relation to urban crime and violence. Weapon involvement and violence is often directly related to the network of crack cocaine users and traffickers. Other crimes, such as

---

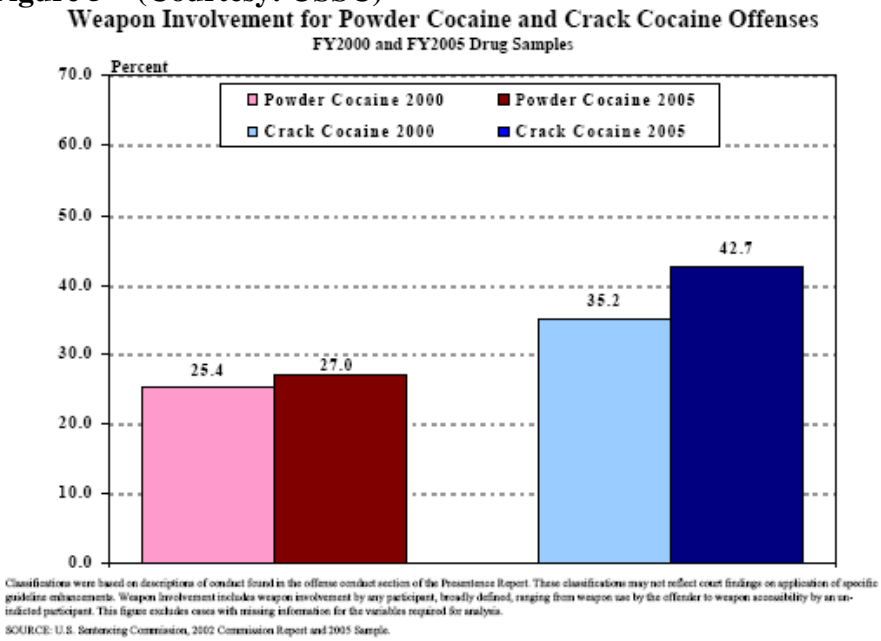
[300] United States Sentencing Commission Report to the Congress: Cocaine and Federal Sentencing Policy. May 2007. 16.
[301] Professor Malo Hutson. Lecture on Oct 8, 2008. "Race and Ethnic Relations, Part 2". UC Berkeley.
[302] Sklansky, David. Stanford Law Review, Vol 47, No 6. July 1995. Cocaine Race and Equal Protection. Pg 1283-1382.

homicide, gang violence, and domestic abuse is, in some studies, correlated to crack cocaine; however, results are largely inconclusive.[303]

Weapon Involvement

Law enforcers use a broad and narrow way to define "weapon involvement". "Broad" includes "weapon involvement in the offense by any participant… ranges from use by an offender to mere access to a weapon by an unindicted coparticipant." The "Narrow" definition only includes offender access, offender possession, or offender use. Detailed data for both definitions are provided in Figures 5 and 6.[304]

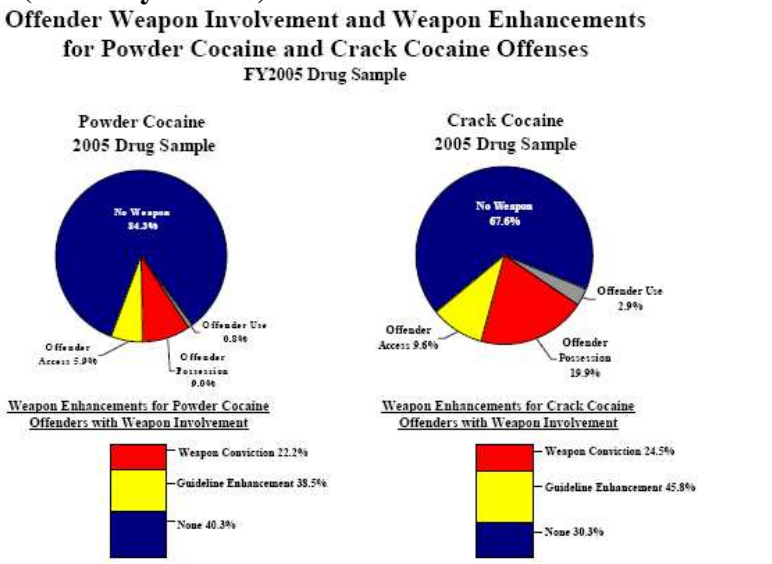
Figure 5 – (Courtesy: USSC)



[303] Grogger, Jeff. NBER Working Paper Series. Introduction of Crack and Rise in Urban Crime Rates. Jan 1998. 1-13.

[304] United States Sentencing Commission Report to the Congress: Cocaine and Federal Sentencing Policy. May 2007. 32-38.

Figure 6 – (Courtesy: USSC)



Classifications were based on descriptions of conduct found in the offense conduct section of the Presentence Report. These classifications may not reflect court findings on application of specific guideline enhancements. The bar charts may sum to more than 100 percent due to the rare occurrence of both a weapon conviction and application of the guideline enhancement. This figure excludes cases with missing information for the variables required for analysis.

SOURCE: U.S. Sentencing Commission, 2005 Sample.

In the year 2005, there was weapon involvement in almost 43% of crack cocaine offenses. In comparison, in the same year, powder cocaine offenses had a 27% rate of weapon involvement. In fact, weapon involvement is the number one crime committed in addition to trafficking/possessing cocaine, followed by violence involvement.[305]

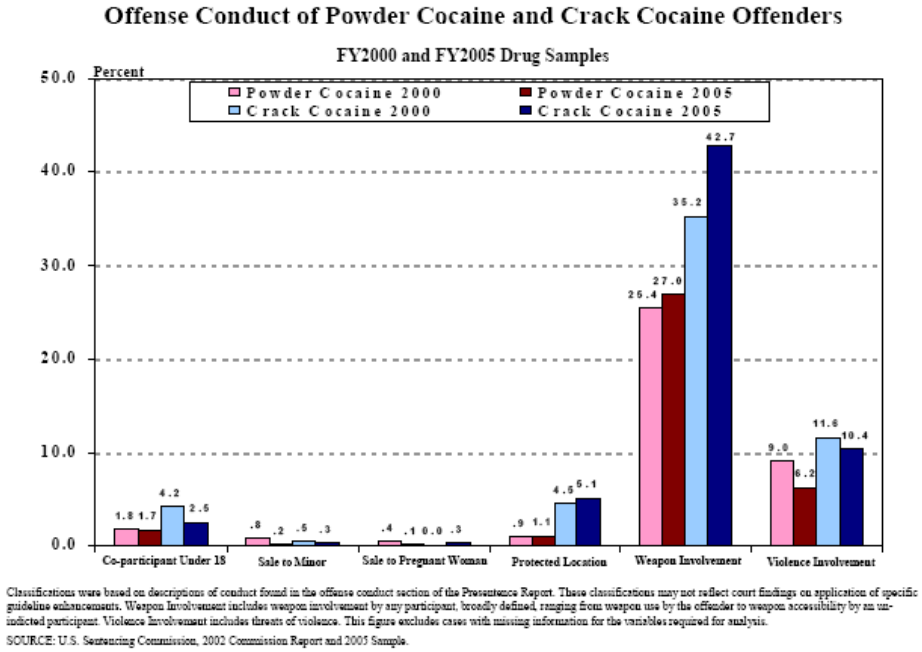
Violence

Law enforcers define violence as death, any injury, or threats. Violence involvement, although the second most common crime associated with crack cocaine, is significantly less prominent than weapon involvement. Violence was associated with crack

[305] Ibid, 38-46.

offenses 10.4% of the time, and with powder 6.2%. See Figures 7 and 8.[306]

Figure 7 – (Courtesy: USSC)

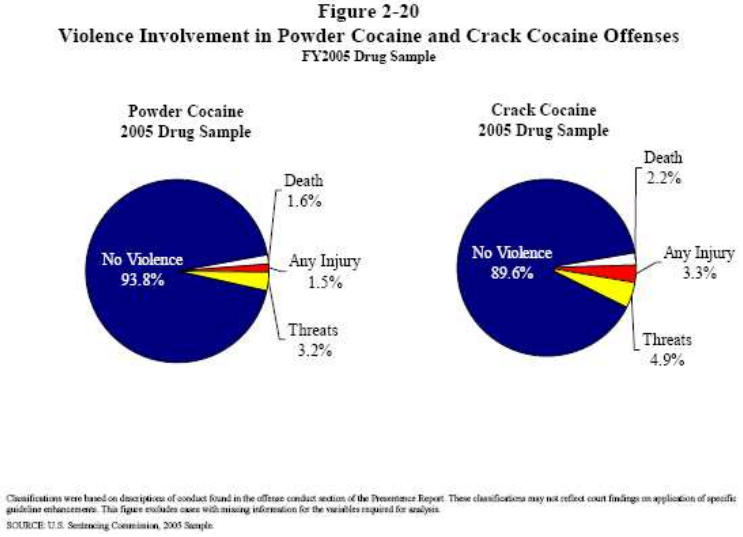


Classifications were based on descriptions of conduct found in the offense conduct section of the Presentence Report. These classifications may not reflect court findings on application of specific guideline enhancements. Weapon Involvement includes weapon involvement by any participant, broadly defined, ranging from weapon use by the offender to weapon accessibility by an un-indicted participant. Violence Involvement includes threats of violence. This figure excludes cases with missing information for the variables required for analysis.

SOURCE: U.S. Sentencing Commission, 2002 Commission Report and 2005 Sample.

[306] Ibid.

Figure 8 – (Courtesy: USSC)



Crimes in addition to and associated with a cocaine-related offense are sentenced separately from the actual cocaine offence. The USSC, in every recommendation to Congress and in its amendment to the 1986 and 1988 Acts, has established harsher penalties for involvement of weapons or violence.

Incarceration

Data regarding the incarceration of black males is staggering. According to the Department of Justice, 3.2% of all black males in the United States are currently serving a prison sentence and the D of J expects 32% of all black males to enter prison at some point during their lifetime[307]. Other studies, such as

[307] US Department of Justice. Office of Justice Programs. Bureau of Justice Statistics. Criminal Offender Statistics. < http://www.ojp.usdoj.gov/bjs/crimoff.htm> Dec 9, 2008.

the one by the Washington-based Justice Policy Institute, claims that there are more black men in jail than in college.[308]

With such staggering data concerning black male imprisonment, organizations such as FAMM, the Sentencing Project, and Crack have blamed this disparity on policies such as the differences in sentencing procedure between powder and crack cocaine.

Conclusion

As the fields of science, medicine, and data analysis advance with time and technology, so do lawmakers' understanding of complicated issues such as drug sentencing policy. In this case, researchers have disproven a common misconception that crack cocaine's pharmacological composition produced more violent and addictive behavior than powder cocaine. However, crime and violence associated with crack is still significantly greater than powder. But one must note that the charges for associated crimes, such as weapons involvement, are sentenced separately than those of trafficking or possession.

Recent trends, such as the allowance by Congress for the Sentencing Commission to reduce the sentencing guidelines for crack cocaine, indicate the direction that the policy governing federal sentencing for crack cocaine is moving towards. However, the lowering of crack cocaine sentencing policy will not help the urban community, specifically the black community, cure itself of the crack cocaine epidemic and the consequences that result from it.

---

[308] BBC News World Edition. August 29, 2002. "More Black US Men in Jail Than in College." <http://news.bbc.co.uk/2/hi/americas/2223709.stm> Dec 9, 2008.

Appendix

Appendix A-1

Demographic Characteristics of Federal Cocaine Offenders
Fiscal Years 1992, 2000, and 2006

	Powder Cocaine						Crack Cocaine					
	1992		2000		2006		1992		2000		2006	
	N	%	N	%	N	%	N	%	N	%	N	%
Race/Ethnicity												
White	2,113	32.3	932	17.8	821	14.3	74	3.2	269	5.6	474	8.8
Black	1,778	27.2	1,596	30.5	1,550	27.0	2,096	91.4	4,069	84.7	4,411	81.8
Hispanic	2,601	39.8	2,662	50.8	3,296	57.5	121	5.3	434	9.0	452	8.4
Other	44	0.7	49	0.9	66	1.2	3	0.1	33	0.7	56	1.0
Total	6,536	100.0	5,239	100.0	5,733	100.0	2,294	100.0	4,805	100.0	5,393	100.0
Citizenship												
U.S. Citizen	4,499	67.7	3,327	63.9	3,463	60.6	2,092	91.3	4,482	93.4	5,195	96.4
Non-Citizen	2,147	32.3	1,881	36.1	2,256	39.4	199	8.7	318	6.6	196	3.6
Total	6,646	100.0	5,208	100.0	5,719	100.0	2,291	100.0	4,800	100.0	5,391	100.0
Gender												
Female	787	11.8	722	13.8	561	9.8	270	11.7	476	9.9	461	8.5
Male	5,886	88.2	4,518	86.2	5,179	90.2	2,032	88.3	4,330	90.1	4,936	91.5
Total	6,673	100.0	5,240	100.0	5,740	100.0	2,302	100.0	4,806	100.0	5,397	100.0
Average Age	Average=34		Average=34		Average=34		Average=28		Average=29		Average=31	

This table excludes cases missing information for the variables required for analysis.

SOURCE: U.S. Sentencing Commission, 1992, 2002, and 2006 Datafiles, MONFY92, USSCFY00, and USSCFY06.

Appendix A-2

2003 Federal Sentencing Guidelines (courtesy: USSC. http://www.ussc.gov/2003guid/tabcon03.htm)

The Sentencing Table used to determine the guideline range follows:

		Criminal History Category (Criminal History Points)					
	Offense Level	I (0 or 1)	II (2 or 3)	III (4, 5, 6)	IV (7, 8, 9)	V (10, 12)	VI 11,(13 or more)
	1	0-6	0-6	0-6	0-6	0-6	0-6
	2	0-6	0-6	0-6	0-6	0-6	1-7
	3	0-6	0-6	0-6	0-6	2-8	3-9
	4	0-6	0-6	0-6	2-8	4-10	6-12
Zone A	5	0-6	0-6	1-7	4-10	6-12	9-15
	6	0-6	1-7	2-8	6-12	9-15	12-18
	7	0-6	2-8	4-10	8-14	12-18	15-21
	8	0-6	4-10	6-12	10-16	15-21	18-24
Zone B	9	4-10	6-12	8-14	12-18	18-24	21-27
	10	6-12	8-14	10-16	15-21	21-27	24-30
Zone C	11	8-14	10-16	12-18	18-24	24-30	27-33
	12	10-16	12-18	15-21	21-27	27-33	30-37
Zone D	13	12-18	15-21	18-24	24-30	30-37	33-41
	14	15-21	18-24	21-27	27-33	33-41	37-46
	15	18-24	21-27	24-30	30-37	37-46	41-51
	16	21-27	24-30	27-33	33-41	41-51	46-57
	17	24-30	27-33	30-37	37-46	46-57	51-63
	18	27-33	30-37	33-41	41-51	51-63	57-71
	19	30-37	33-41	37-46	46-57	57-71	63-78
	20	33-41	37-46	41-51	51-63	63-78	70-87
	21	37-46	41-51	46-57	57-71	70-87	77-96
	22	41-51	46-57	51-63	63-78	77-96	84-105
	23	46-57	51-63	57-71	70-87	84-105	92-115
	24	51-63	57-71	63-78	77-96	92-115	100-125

25	57-71	63-78	70-87	84-105	100-125	110-137
26	63-78	70-87	78-97	92-115	110-137	120-150
27	70-87	78-97	87-108	100-125	120-150	130-162
28	78-97	87-108	97-121	110-137	130-162	140-175
29	87-108	97-121	108-135	121-151	140-175	151-188
30	97-121	108-135	121-151	135-168	151-188	168-210
31	108-135	121-151	135-168	151-188	168-210	188-235
32	121-151	135-168	151-188	168-210	188-235	210-262
33	135-168	151-188	168-210	188-235	210-262	235-293
34	151-188	168-210	188-235	210-262	235-293	262-327
35	168-210	188-235	210-262	235-293	262-327	292-365
36	188-235	210-262	235-293	262-327	292-365	324-405
37	210-262	235-293	262-327	292-365	324-405	360-life
38	235-293	262-327	292-365	324-405	360-life	360-life
39	262-327	292-365	324-405	360-life	360-life	360-life
40	292-365	324-405	360-life	360-life	360-life	360-life
41	324-405	360-life	360-life	360-life	360-life	360-life
42	360-life	360-life	360-life	360-life	360-life	360-life
43	life	life	life	life	life	life

Works Cited

Drug and Alcohol Services Information System. “The DASIS Report”. February 25, 2005.

Federal Sentencing Reporter, Vol 14. No. 3-4. 2001-2002. US Sentencing Commission Hearing 2/25/02: Cocaine Pharmacology, Crack Babies, Violence.

Frieden, Terry. “Mukasey Wants Police Support to Prevent Prisoner Releases”. Feb 26, 2008, CNN.com. <http://www.cnn.com/2008/CRIME/02/25/cocaine.sentencing/> Dec 1, 2008.

Fryer, Roland. National Bureau of Economic Research. Measuring the Impact of Crack Cocaine. May 2005.

Grogger, Jeff. NBER Working Paper Series. Introduction of Crack and Rise in Urban Crime Rates. Jan 1998.

Hutson, Professor Malo. Lecture on Oct 8, 2008. “Race and Ethnic Relations, Part 2”. UC Berkeley.

National Public Radio Website. Nov 2, 2007. US Sentencing Ranges Lowered for Crack Cocaine. Nov 30, 2008.

Sentencing Resource Counsel. Nov 1, 2007. “Applying the Crack Amendments 101.”

Sklansky, David. Stanford Law Review, Vol 47, No 6. July 1995. Cocaine Race and Equal Protection.

Supreme Court of the United States. Slip Opinion, Syllabus. October Term 2007. December 10, 2007. Kimbrough v. United States. Dec 5, 2008.

United States Sentencing Commission. An Overview of the Federal Sentencing Guidelines. Pg 3. <http://www.ussc.gov/2003guid/tabcon03.htm>

United States Sentencing Commission. Final Report on United States v. Booker On Federal Sentecing. March 2006.

United States Sentencing Commission Report to the Congress: Cocaine and Federal Sentencing Policy. May 2002.

United States Sentencing Commission Report to the Congress: Cocaine and Federal Sentencing Policy. May 2007.

USSC. Public Hearing on Cocaine Sentencing Policy. November 14, 2006.

Watts, J.C., Washington Times. Feb 12, 2008. "Reforming Crack Cocaine Law". <http://www.washingtontimes.com/news/2008/feb/12/reforming-crack-cocaine-law/> Nov. 29, 08.

The Road to Transparency:
China's Response to Environmental Degradation

By Tod Kaiser

Introduction

Despite China's existence as an authoritarian state, the government's grip over the country is not as strong as it appears. While the Tiananmen Square massacres of 1989 were a reminder of the potential strength as well as brutal tactics the Chinese Communist Party (CCP) has on hand, that same strength is largely confined to dealing with isolated incidents within city limits, as was the case in Beijing—China's capital and CCP military stronghold. Naturally, the Chinese government called in the People's Liberation Army, dealing swiftly and surely with the thousands of pro-democracy student protestors lacking the fortune to be safe in their dormitories far from the Square the morning of June Fourth. However, because China is such a large and vast country, if protests of an equal or slightly lesser magnitude were to occur all over the country en masse, the Chinese government would not have the capacity to deal with these nationwide protests, be subsequently overwhelmed, and possibly overthrown. This scenario is what Chinese leaders fear most—being overthrown—and it is the fear of multiple "Tiananmen incidents" occurring throughout the country that has incentivized China's leaders to create policies that help to legitimize their rule. Those policies are, not surprisingly, to deliver high economic growth rates with the goal of maintaining social stability—creating a "harmonious society."

China's economic growth and development over the past few decades has struck awe in those who have visited its megacities and manufacturing centers. From glitzy skyscrapers in Shanghai to the busy local village textile factories in Guangzhou, economic activity is and can be seen nearly everywhere in the country. Maintaining staggering gross domestic product outputs until only recently this past year, China has achieved average growth rates that leaders in the developed world could only dream of. In little over a generation, by creating policies conducive to

economic growth and development, China's government has been able to successfully lift half a billion of its citizens out of poverty.[309] This feat can be seen as one of humanity's greatest achievements in the past century. In spite of delivering high economic growth rates that have created jobs and opportunities for many, the goal of maintaining social stability is currently under question, for the achievements of economic growth and development come with a flip side. Vast problems plague the country—one of which is horrendous environmental degradation. It is unfortunate that the very same economic and development policies that have transformed China into the world's factory have also turned it into one of the world's biggest polluters.

China is a land of many "firsts"—first in the world in terms of population, first in the world in terms of gold medals won at the 2008 Summer Olympics, and also first in the world in terms of carbon emissions. According to the Netherlands Environmental Assessment Agency, in 2006 China surpassed the United States as the world's number one carbon emitter by a margin of 8 percent.[310] Much of these carbon emissions are produced in coal-fired power plants, which generate roughly 70 percent of the nation's energy supply.[311] As cheap as coal is, it is also one of the dirtiest sources of energy. Coal-induced air pollution has become so severe that ambient air pollution is blamed for incurring hundreds of

---

[309] David Dollar, "Poverty, inequality and social disparities during China's economic reform," World Bank, 2007, http://www-wds.worldbank.org/external/default/WDSContentServer/IW3P/IB/2007/06/13/0000164
06_20070613095018/Rendered/PDF/wps4253.pdf.

[310] Brad Knickerbocker, "China now world's biggest greenhouse gas emitter," *The Christian Science Monitor*, June 28, 2007, http://www.csmonitor.com/2007/0628/p12s01-wogi.html.

[311] Volker Mrasek, "China's Greenhouse Gas Emissions Threaten to Double," *Spiegel Online International*, March 6, 2009, http://www.spiegel.de/international/world/0,1518,611818,00.html.

thousands of deaths per annum, with only 1 percent of China's 560 million urban dwellers breathing air considered safe by the European Union.[312] As dirty as coal is, the energy generated from it powers the chemical and manufacturing industries needed to sustain China's high economic growth rates. Though highly profitable, these same industries—many of which are located near lakes and rivers—generate considerable amounts of water pollution. It is estimated that between 300 and 500 million Chinese lack access to clean piped water.[313] Of these, nearly 200 million drink water that is making them ill, and roughly 30,000 children die each year from drinking contaminated water.[314] More than 70 percent of all rivers and lakes in China are polluted, with more than half of all urban groundwater contaminated.[315] China's Ministry of Environmental Protection (MEP) estimates in their *Official 2007 Report on China's Environment* that all seven of the country's major rivers suffer moderate pollution, and that 11 out of 28 major lakes have water quality unsuitable for any usable purpose.[316] It is without a doubt that China is in the midst of an environmental crisis.

---

[312] Joseph Kahn and Jim Yardley, "As China Roars, Pollution Reaches Deadly Extremes," *The New York Times*, August 26, 2007, http://www.nytimes.com/2007/08/26/world/asia/26china.html?_r=1&pagewanted=all.

[313] World Bank, *Cost of Pollution in China: Economic Estimates of Physical Damages,* 2007, http://siteresources.worldbank.org/INTEAPREGTOPENVIRONMENT/Resources/China_Cost_of_Pollution.pdf, 33.

[314] Organization for Economic Co-Ordination and Development, *OECD Environmental Performance Reviews: China*, Volume 24, 2007, 239.

[315] Zhang Ke, "Group Monitors China's Water Polluters Using Online Mapping," World Watch Institute, 2006, http://www.worldwatch.org/node/4622.

[316] Ministry of Environmental Protection, *Official Report on China's Environment,* (in Chinese), *2007*, http://www.chinaenvironment.com/uploads/454/2008-8-25/1.pdf.

What can be done to help address China's ongoing environmental catastrophe, especially its horrendous water pollution? Those in the Western world are quick to point out that one of the most effective ways to bring polluters accountable is by engaging and increasing participation among citizenry through transparency mechanisms. However, there are significant barriers to citizen participation in China, the most notable being that China is not a free society. In 2008, Freedom House rated China as one of the world's worst nations when it comes to freedom of information and disclosure.[317] Censorship is abundant, and the government controls nearly every aspect of information dissemination in society, ranging from blocking websites deemed politically threatening to the censoring of key words being sent in mobile text messages.[318] When citizens ask or press for environmental performance investigations on suspected polluting industries, often they are turned away or arrested by local government officials on accusations of instigating social instability. This tradition of censorship and information secrecy has created an inability on the part of China's citizenry to peacefully address their concerns and grievances over their environment and to hold polluters accountable through legal and bureaucratic means. Lacking effective institutional channels to hold polluters accountable, Chinese citizens are taking their grievances to the streets.

Chinese citizens are not standing by passively as their environment denigrates. Throughout China, there have recently been increasing environmentally (mostly water pollution) related protests by outraged citizenry demanding a clean and healthy environment, many of which have ended in violence. Party leaders are concerned that these protests are creating social instability, as

---

[317] Freedom House, *Freedom in the World—China,* 2008, http://www.freedomhouse.org/inc/content/pubs/fiw/inc_country_detail.cfm?year=2008&country=7372&pf.

[318] Ibid.

well as setting the stage for another "Tiananmen," the dread of any Chinese political leader. It is because of this fear that Chinese leaders are searching for effective ways to mitigate these protests.

The very same year Freedom House published their report, on May 1, China's State Council (China's cabinet) promulgated Open Government Information Regulations (OGI), requiring all levels, branches, ministries, and agencies of government to create their own implementing measures. OGI is essentially equivalent to a freedom of information act commonly found in many democratic governments. The regulations give Chinese citizens the right to receive government-held information upon request as well as increase efforts to publicize information already available. China now joins the ranks of only 70 nations to have implemented similar legislation.[319] The same day OGI was passed, the Ministry of Environmental Protection (MEP), which is delegated responsibility for improving and safeguarding China's environment, began implementation of Measures on Open Environmental Information (OEI). As required under the broader OGI regulations, OEI measures will implement aspects of OGI as pertaining to the environmental realm, creating transparency and accountability by giving citizens the legal right to request environmental information.[320] The recent passing of OEI in China begs the following question: why would an authoritarian government self-regulate by placing itself under the scrutiny of the public?

---

[319] Gang He, "Freedom of Information and Environmental Protection in China," *Earthtrends,* July 28, 2008, http://earthtrends.wri.org/updates/node/324.

[320] Environmental information, as defined in OEI, is any kind of information—government or business held—that deals with any aspect or relation to the environment. For example: pollution data, laws, regulations, planning standards, procedures, fines, lists of severely polluting industries, and other government service information. For more information, please see Articles 2 an 11 of OEI (*Measures on Open Environmental Information, 2007)* and Gang He's "Freedom of Information."

This paper is formed around the idea that the Chinese government, by necessity, has created OEI in response to rising social instability caused by horrendous environmental degradation. To better understand the context and dynamics from which OEI came into existence, as well as highlight potential challenges facing OEI's implementation, this paper is organized into four sections. *Section 1* highlights the severity and destabilizing nature of environmentally related protests and riots, or as government officials use the euphemistic term "environmental mass incidents," as having forced China's leaders to create viable channels for civil society to hold polluters and corrupt officials accountable. *Section 2* reveals that the notion of increasing public participation by publicizing environmental information has been on the Chinese government's policy agenda for quite some time, with experimental policies in the form of pilot projects stretching as far back as 1998. By examining the results of each pilot project did China's government increase its confidence in publicizing environmental information, giving rise to OEI. *Section* 3 examines key components of OEI and the potential the measures have to effectively mitigate environmental degradation. Finally, *Section* 4 acknowledges that though OEI looks very promising, it still faces many hurdles concerning proper consistent national enforcement.

Section 1: Rising Instability—Environmental Mass Incidents

The growing number of disputes, protests, and even riots is symptomatic of China's worsening environmental situation. The exact statistics on the numbers of "environmental mass incidents" (*huanjing qunti xing shijian*) in China are a bit ambiguous, but it is estimated that 5,000 incidents occurred in 2004 and that ever since then, the numbers have been increasing steadily by roughly 30

percent every year.[321] These numbers are alarming and point to the significant social instability crisis the Chinese government is facing. One notable environmental mass incident occurred in the city of Dongyang, Zhejiang Province in April of 2005. In *Foreign Affairs*, Elizabeth Economy highlights the violence of the Dongyang protest:

> After trying for two years to get redress by petitioning local, provincial, and even central government officials for spoiled crops and poisoned air, in the spring of 2005, 30,000-40,000 villagers from Zhejiang Province swarmed 13 chemical plants, broke windows and overturned buses, attacked government officials, and torched police cars. The government sent in 10,000 members of the People's Armed Police in response. The plants were ordered to close down, and several environmental activists who attempted to monitor the plants' compliance with these orders were later arrested.[322]

The Dongyang case is a classic example of how pollution incidents that have not been settled early on only increase in severity over time. When a certain threshold is crossed, the public is forced to take their concerns and grievances to the streets. At first glance, two years of petitioning to all levels of government without yielding positive results would seem ample time for public discontent to reach the point of igniting violence.[323] On the contrary, similar to how other environmental mass incidents

---

[321] Tianjie Ma, "Environmental Mass Incidents in Rural China: Examining Large-Scale Unrest in Dongyang, Zhejiang," *China Environment Series,* Issue 10, 2008, 33.

[322] Elizabeth Economy, "The Great Leap Backward?" *Foreign Affairs*, September/October, 2007, http://www.foreignaffairs.org/20070901faessay86503/elizabeth-c-economy/the-great-leap-backward.html ?mode=print, 4.

[323] Ma, "Environmental Mass Incidents," 39.

develop in China, events leading up to Dongyang go back even further in time.

Ma Tianjie's article in *China Environment Series* documents in detail the chronological progression of the Dongyang incident.[324] He writes that public discontent began to surface when plots of land near two villages in Dongyang were designated to be the site of a chemical industrial zone in 1999.[325] The deal was arranged by revenue-seeking local government officials offering relaxed land use regulations to attract investment.[326] From a revenue standpoint, the deal was financially lucrative: "By 2004, 13 chemical companies had moved into the area, producing products [ranging] from herbicides to plastic products and generating a combined annual revenue of approximately 200 million Yuan (~25 million)"[327] However, the revenue generated from the chemical plants did not deter local villagers from voicing their pollution concerns.

Wang Wei, a party secretary from one of the local villages near the chemical industrial zone, openly disagreed with the revenue generating scheme upon further examination of the chemical plants moving in. In 2001, when Dongnong Pesticide Company agreed to settle in the zone, Wang took initiative by leading a personal investigation into the company, recording his findings in an article he titled "A Portrait of Dongnong."[328] In the article, he tracked the company's notorious record for emitting horrendous amounts of pollution, pollution so bad that it was revealed the company was forced out of other villages prior to settling in Dongyang.[329] Armed with over a thousand printed

[324] Ibid., 38-40.
[325] Ibid., 39.
[326] Ibid.
[327] Ibid.
[328] Ibid.
[329] Ibid.

copies of his findings, Wang began a campaign to inform villagers on their new polluting neighbor. Through his efforts, awareness of Dongnong's pollution history increased. Despite good intentions, his campaign backfired, becoming a political miscalculation: his pamphlets sparked public outrage towards the chemical plant, with brief acts of violence leading to the wounding of a local government official and the destruction of some factory equipment. [330] After being held by authorities, Wang and 11 other villagers were given prison sentences of up to three years.[331] And in spite of these nascent displays of violence, significant amounts of pollution from the pesticide company would only increase.

A torrent of untreated wastewater from the chemical plants continued to be discharged into nearby rivers, the very same rivers that served as the main source of water for the villagers' crops.[332] In July of 2003, the entire rice crop produced by one local village was destroyed, ruined by chemical runoff. As Ma Tianjie writes, "The damages to local agriculture were so serious that farmers had to buy more expensive vegetables from urban areas [just] to feed their families."[333] In addition to facing shortages of food, villagers suffered other health complications from gas emissions leaking out of the chemical plants—affecting vision by irritating the eyes.[334]

The combination of food scarcity combined with health problems compelled villagers to make multiple attempts to use the existing "complaint system" (*xinfang*) channels to petition environmental protection bureaus (EPBs) at the local (Dongyang), prefecture (Jinhua), and provincial (Zhejiang) levels.[335] Most of the villagers' complaints were ignored—there was one instance where

[330] Ibid.
[331] Ibid.
[332] Ibid.
[333] Ibid.
[334] Ibid.
[335] Ibid.

a reply from the Zhejiang EPB indicated that some chemical companies "were violating the rules."[336] In spite of this acknowledgement, no attempts were made to stop the operations of the factories. Failing to seek redress using existing channels, some villagers—albeit unsuccessful—turned their attention to the media. In early 2005, one villager by the name of Wang Zhongfa tried to recruit journalists in Beijing to publicize the worsening environmental conditions in Dongyang. However, his actions would only lead to an outcome too often experienced by many Chinese environmentally concerned leaders. Similar to party secretary Wang Wei's fate, Wang Zhongfa would later be arrested on accusations of instigating social unrest on April 6, 2005.[337]

In March of 2005, villagers rallied to confront the mayor of Dongyang in person, but to no avail.[338] The culmination of failures from previous attempts to address their grievances through the complaint system, combined with this latest refusal proved too great for the villagers: the tipping point had been reached. Determined, a series of bamboo shelters were constructed to stop the flow of traffic through the industrial zone. Local government officials and police in turn responded by raiding the protesters and burning a handful of the ad hoc structures. Tolerating the raids, the villagers remained. A few days later, the Dongyang government issued edicts calling for all thirteen chemical plants in the industrial zone to halt production momentarily to make "adjustments" (*tingchan zhengdun*).[339] By this time the villagers had lost all trust in their government, and still remained.

The police continued to raid and make arrests throughout all of March and into early April. On April 10, government officials tried to break up the protesters by amassing thousands of

[336] Ibid.
[337] Ibid.
[338] Ibid.
[339] Ibid.

police and government employees to forcibly remove the bamboo structures blocking the road.[340] Ma Tianjie notes that the attempted forced removal merely fanned the flames of anger, provoking an even stronger resistance from the villagers, turning into a riot.[341] Thousands more joined in support of the villagers, and it was fortunate that no one was killed, though dozens were injured, some severely.[342] Yet still the authorities could not clear the blockade; it was reported that many authorities fled the scene.[343]

Given the cataclysmic nature and scale of the Dongyang environmental mass incident, it was inevitable that the case would receive much publicity, capturing the attention of the central government. The Ministry of Environmental Protection (MEP) led a team to investigate the industrial zone.[344] Upon inspection, MEP ordered Dongnong Pesticide, along with other highly polluting companies, to immediately cease operations and vacate the industrial zone. Wary of empty government promises, the villagers remained with vigilance, waiting for observable government action. As Ma Tianjie concludes his detailed account of the Dongyang case, he describes the resilience of the protestors: "Only on May 20, after seeing the machinery from the factories removed the week before, did the villagers finally take down the tents."[345]

Dongyang represents a typical environmental mass incident whereby citizens, fed up with bureaucratic inaction, ineptness and unwillingness to listen to their grievances, took matters into their own hands and protested as a last resort. This incident highlights what happens when a government does not listen to the concerns of its citizens and lacks effective institutional mechanisms to make

[340] Ibid., 40.
[341] Ibid., 40.
[342] Ibid., 40.
[343] Ibid., 40.
[344] In 2008, the State Environmental Protection Administration (SEPA) restructured to ministerial level, becoming MEP.
[345] Ma, "Environmental Mass Incidents," 40.

polluters and corrupt local officials accountable. The significance of the Dongyang case lies not in what government officials accomplished, but what government officials failed to accomplish: transparency.

China's leaders are viewing transparency as key to providing a channel for citizens to voice their concerns and grievances to a government that successively listens to them. Transparency allows the public to voice their concerns in projects that have environmental consequence early on, even before projects have any environmental impact. By providing more opportunities for early environmental information disclosure and early public involvement in planning and resolving conflicts, transparency can serve to ease pressure, as well as decrease the rising number of environmental mass incidents by holding polluters and corrupt officials accountable.

The Chinese central government realizes the potential of transparency and has thus called upon MEP to enforce the Measures on Open Environmental Information (OEI). However, OEI did not materialize out of thin air simply in response to the increasing number of environmental mass incidents. Rather, the concept of open environmental information disclosure to mitigate pollution has been on the central government's agenda list for quite some time, with experiments in the form of pilot projects going as far back as 1998.

Section 2: Pilot Projects and the Road to Transparency

Deng Xiaoping's phrase "crossing the river by feeling the stones" (*muozhe shitou guo he*) embodies the conservative approach China has taken with regard to implementing new policies. Similar to its incremental economic reform policies beginning in the late 1970s, China has used a gradualist approach towards the development of OEI, keeping experimentation local rather than on a national scale. The results of the following pilot

projects document the increased confidence among Chinese leaders in adopting progressive policies to improve transparency. All three pilot projects are unique in the sense that each one was groundbreaking. The first case involves the disclosure of air pollution reports for the first time in China's major cities. The second case involves publicizing for the first time environmental performance ratings of companies, and the third incident involves for the first time a public hearing to create active public participation.

Air Pollution Reporting

Although many cities across China have monitored air pollution for decades, information was never published until the late 1990s. The government's reasoning at the time is revealed in the following *New York Times* article: "For 20 years, local officials carefully measured [Beijing's] air pollution levels and equally carefully hid the results—fearing that the truth might tarnish the capital's image or lead to social unrest."[346] This line of reasoning is further elaborated in the following quote by a Shanghai official: "If we simply release the information to the public, the disadvantages would outweigh the advantages….They may say, 'The government did a bad job. Why did you give us such bad air?' "[347] The concern of this official is representative of pre-1998 thinking, whereby government officials did not want the public release of air quality information. These officials feared that published data would provoke an otherwise avoidable backlash by concerned environmentally conscious citizenry, which could then lead to

[346] Elisabeth Rosenthal, "China Officially Lifts Filter on Staggering Air Pollution Data," *The New York Times*, June 14, 1998, http://www.nytimes.com/1998/06/14/world/china-officially-lifts-filter-on-staggering-pollution-data.html.

[347] US Embassy-China, "The Fading of Chinese Environmental Secrecy," *US Embassy-China webpage*, 1998, http://www.usembassychina.org.cn/english/sandt/chplca/htm.

social instability. However, according to Gang He, a research associate at Stanford University's Program on Energy and Sustainable Development, some far-sighted leaders insisted on the releasing of air quality information for large cities in the form of weekly reports.[348] These progressive-minded officials represent a new line of thinking in the Chinese government, believing that the old ways of hiding reports merely fostered a culture of increased distrust among the Chinese people towards their government. Like many new policies that are introduced in China, in 1998 the air pollution reports were released in incremental fashion, limited in the beginning to a handful of select cities, such as Beijing. By 2005 over forty-six cities were publishing air pollution reports.[349]

Despite initial insecurity on the part of officials, since 1998 millions of people everyday throughout China can read, watch, or hear air pollution reports of large and small cities published in newspapers, the Internet, television, or the radio.[350] The response to the air quality reports has not resulted in rising social instability as was initially feared. Rather, the transparency created has had the effect of raising the public's consciousness and trust with their government. According to a Beijing environmental official, "releasing the numbers [was] a revolutionary concept for the people and the government. We were worried that people would complain that air pollution is too serious. Instead, the consciousness of people has been raised. And they feel the government trusts them with the facts, so we are gaining points by doing this."[351] With public consciousness raised, the Chinese government has also had the benefit of being exposed to

[348] He, "Freedom of Information."
[349] Steven Andrews, "Seeing Through the Smog: Understanding the Limits of Chinese Air Pollution Reporting," *China Environment Series*, Issue 10, 2008, 6.
[350] Ibid., 5.
[351] Rosenthal, "China Officially Lifts Filter."

constructive pressure, as the air quality reports have catalyzed movements to improve air quality. For example, in light of air quality reports, Beijing has promised more "blue sky" days—days of considerably lesser air pollution—by earmarking more than 140 billion RMB (~$20.4 billion) in funds to help make that promise become reality.[352] Not only did Beijing try to immediately reduce pollution in preparation for the Olympic Games, the city also made a genuine attempt to provide healthy air as an added long-run benefit to its residents.[353]

The significance of examining the public release of air pollution reports is that the people place trust in a government that in turn places trust in the people. Viewing these reports as an act of honesty on the government's account has served to raise the esteem of the government by its honest actions and candor. Public disclosure of information has served to increase environmental consciousness and awareness, fostering a space for constructive dialogue between government and citizen rather than by fostering a feeling of mutual distrust. Moreover, government action in reducing air pollution, evinced by Beijing's investment of $20.4 billion in sustainable infrastructure and technologies to clean the air, further helps to create accountability on the government's side and trust among its citizens.

Environmental Performance Information Disclosure

Tsinghua University professor Wanxin Li writes in *China Environment Series* on how in 1999 the Chinese government launched a pilot project in Zhenjiang, Jiangsu Province to increase transparency and citizen participation through "environmental

[352] He, "Freedom of Information."
[353] Ibid.

performance information disclosure" (EPID).[354] The function of EPID was to rate the environmental performance of industries using a color-coded scale—green, blue, yellow, red, and black—whereby green was the best and black the worst, respectively.[355] These ratings were then to be made public to the news media.[356] The idea was that by revealing the environmental ratings of companies caught violating pollution standards, the public would be empowered to target polluters and pressure EPB officials to take action. In Zhenjiang, the EPID pilot project was extensively implemented to great success. Since coming into operation in 1999, in 2000 there were nearly 91 companies which received color-coded ratings. In 2005, company participation increased to 800.[357] The example below illustrates one particular success story.

In 2002, a local construction materials manufacturer received the worst rating: "black."[358] This information was made available to the public as was required under EPID. The CEO of the blacklisted company faced considerable shame from not only the public, but also friends at the dinner table. Fearing that not only his image but the company's image would be tarnished, the CEO decided to invest in wastewater treatment. In 2003, the same company that was rated "black" just the previous year raised its rating to "blue."[359] In this case, both pubic and private scorn reflected poorly upon the company, and because it wanted to preserve its image, the company changed its habits and reduced its pollution.

---

[354] Wanxin Li, "Opening up the Floor: Environmental Performance Information Disclosure Pilot Programs in Zhenjiang and Hohhot," *China Environment Series,* Issue 8*,* 2006, 125-129.
[355] Ibid., 125.
[356] Ibid.
[357] Ibid.
[358] Ibid., 128
[359] Ibid.

The key to understanding the Zhenjiang case is that the public disclosure of pollution information impelled the company to reduce its water pollution discharges. This case also highlights how the government did not have to tell the company to do anything with regard to reducing pollution. Just the mere publicizing of negative information was enough to catalyze efforts to reduce pollution on the company's part. It is safe to assume that had information not been made public, the company would have continued to discharge untreated wastewater.

Zhenjiang demonstrates yet again another instance whereby public disclosure of information did not lead to a backlash from outraged citizens. Overall, the release of environmental information helped raise public awareness on environmental issues as well as bring a polluter to change its habits. However, simply publicizing information is not enough. According to Wanxin Li, information that is publicized does not necessarily mean that the public will take action to hold polluters accountable.[360] Though the color-coded results were published in local newspapers and on the Internet, no effort was made to actively engage the public by means of public education programs or to teach citizens on matters of interpretation.[361] In 2000, Nanjing Univerity conducted a survey in Zhenjiang on the EPID program, revealing that only 56 percent of 845 respondents knew of the program's existence, with only 8.3 percent understanding its purpose.[362] As the survey indicates, the simple release of environmental information will not live to the fullest potential unless information released is combined with proactive public engagement.

---

[360] Ibid., 128.
[361] Ibid.
[362] Dong Cao, Genfa Lu, Hua Wang, and Jinnan Wang, *Environmental Information Disclosure: Theory and Practice*, Beijing: Chinese Environmental Science Publisher, 2002.

Yuanmingyuan (Old Summer Palace) Public Hearing

Yuanmingyuan differs from pilot projects strictly publicizing air quality and environmental performance ratings in the sense that it represents the first case whereby proactive public engagement occurred. In an article by Allison Moore and Adria Warren in *China Environment Series*, they describe the case.[363]

In March 2005, a visiting Lanzhou University professor noticed that park officials were engaging in a massive construction project that would cover the lakebeds in Beijing's Old Summer Palace with plastic and cement. The rationale behind this action was to prevent drainage, as the lakes are seasonally dry nine months a year. Believing that the construction project would greatly compromise the surrounding ecosystem, the professor exposed the project on a website, sparking widespread national attention and concern.[364]

As public outcry rapidly increased, both the Beijing and Haidian District EPBs promptly investigated and came to the conclusion that the project was not following environmental impact assessment guidelines. On April 7, 2005, MEP (then SEPA) announced for the very first time that a public hearing would convene, inviting interested members of the public to apply. After four days, 73 out of 200 applicants were selected to be public representatives, receiving an invitation to attend the hearing. These representatives reflected a broad and highly diverse group: park officials, Beijing government officials, scholars (including the Lanzhou professor), businesses, students, engineers, and other professionals.[365]

---

[363] Allison Moore and Adria Warren, "Legal Advocacy in Environmental Public Participation in China: Raising the Stakes and Strengthening Stakeholders," *China Environment Series*, Issue 8, 2006, 5-10.
[364] Ibid., 8-9.
[365] Ibid., 9.

On April 13, all of the representatives gathered to determine (1) if the project failed to protect the ecology of the lakes, (2) review expert opinions on the project to see if it was based on true science, and (3) decide if construction already completed ought to be removed.[366] After long debates, deliberations, and hearing the concerns of citizens and expert opinions, the representatives reached a conclusion. The public hearing results and recommendations stated that the project was ecologically unfriendly and that there were alternative sustainable solutions other than layering the lakebeds with plastic and cement. The representatives also called for an immediate halt to the project and the removal of all completed construction.[367] Upon receiving the results and recommendations, MEP decided to partially comply, citing that because the project was nearly 90 percent complete, a total dismantling of the project's already $4.6 million incurred sunk costs would be too costly, and would not be politically favorable. Therefore, MEP compromised by declaring that construction was to be halted, with partial dismantling of already constructed sections.[368]

The success of Yuanmingyuan rests not on whether an environmentally favorable outcome was reached per se; rather, the case represents a success in generating genuine public participation. By requiring a public hearing (though not mandatory by law), MEP took a step further by creating a space for which constructive dialogue could occur between the public, experts, businesses and government.[369] This case, according to Allison Moore and Adria Warren, serves as a model example of how the direct conflict between public opinion and government decision-makers can take place in an orderly fashion without instigating

[366] Ibid.
[367] Ibid., 10.
[368] Ibid.
[369] Ibid., 5.

social instability.[370] The government did nearly everything right in handling the environmental controversy over Yuanmingyuan.

Yuanmingyuan can also be seen as a case where the highest degrees of transparency was displayed. First, the government did not abstain from listening to the public, as was in the case of Dongyang. Second, the government even went so far as to voluntarily hold a public hearing, thus allowing the direct participation of stakeholders and decision makers to formulate a recommendation. Therefore, the significance of Yuanmingyuan lies not in the recommendation itself, but the very process by which the recommendation came about. Throughout the entire public hearings process, no environmental information was withheld, and all opinions were accounted for. It is the process of actively engaging the public that Chinese leaders seek to use in helping to mitigate environmentally controversial projects.

Looking back at all three pilot projects, the Chinese government came to grips with the reality that releasing environmental information did not create outrage among citizens to the point where social instability arose. Rather, the very act of publicizing environmental information led to a positive impression of government on the part of citizens. At the same time, the releasing of public environmental information even led to efforts mitigating some pollution, as was seen with the CEO's actions when his company was given a publicized rating of "black." The experiment of a public hearing by MEP in the Yuanmingyuan case illustrated orderly public participation in its highest form by physically gathering stakeholders and decision-makers together to discuss the environmental issue at hand. All of the aforementioned pilot projects resulted in a positive effect, and in some form or another led to a mitigation or at least step forward towards pollution mitigation. The results of the pilot projects at the regional levels gave China's leadership the confidence to take the

[370] Ibid., 10.

transparency policies of the pilot projects and package them on a national scale, culminating in the passing of Open Environmental Information (OEI).

Section 3: The Potential of OEI

OEI is the compilation of the successful transparency strategies employed by the Chinese government in its previous pilot projects. What makes OEI so important is that it is a nationalized program that has institutionalized transparency, and it has made transparency a right. According to Gang He, OEI gives citizens the legal right to request environmental information from MEP and its provincial subdivisions, the local EPBs.[371] This marks a major shift in thinking by the government in the sense that the publicized disclosure of environmental information prior to OEI was approached as a privilege from government to citizen. This is not the case anymore, as OEI has gone a step further and made access to environmental information a citizen right. By instituting provisions for a legal framework from which the government can work with, this essentially can be seen as China's attempt to institute rule *of* law rather than rule *by* law.

OEI emphasizes specificity by setting clear provisions and guidelines for what is deemed environmental information and the procedure for its disclosure. As Gang He mentions, OEI elucidates the scope of information deemed "environmental," giving over seventeen different kinds of environmental information.[372] These refined definitions and categorizations—listed in Article 11—of what is environmental information and what is not environmental information serve to dispel potential ambiguity and to provide clarity in the disclosure process. Government officials are subsequently given fewer options to deny requests for information. In addition to refining definitions, OEI requires local EPBs to

[371] He, "Freedom of Information."
[372] Ibid.

publicize all environmental information collected. This is further enforced by the notion of citizens' rights to access information, even if information is not disclosed on the EPB's own initiative. The mandates for full disclosure combined with citizens' rights of access to that information, though they may overlap in purpose, serve to provide greater confidence that environmental information is actually accessed.

An important component of OEI is its requirement for businesses caught violating pollution standards. Local EPBs, which maintain the lists of polluting businesses, are required to publicize the lists of polluters. Upon release, Article 20 requires blacklisted enterprises to provide environmental impact assessments of their operations within thirty days to the public.[373] Included in the environmental information is as follows:

> (1) [Business] name, address and legal representative; (2) Name of major pollutants, method, content and total volume of emission, information on emission that has surpassed the standards or total emission that has surpassed the prescribed limits; (3) Information on the construction and operation of its environmental protection facilities; and (4) Emergency plans for sudden environmental pollution accidents....Enterprises shall not refuse to disclose environmental information referred to in the above paragraph under the excuse of confidentiality of trade secrets.[374]

The significance of Article 20 is that companies with a record of violating pollution standards can no longer resist investigations on grounds of "trade secrets," such as how the companies produce their profits. This provision increases confidence that businesses

---

[373] State Environmental Protection Administration of China, *Measures on Open Environmental Information (for Trial Implementation),* 2007, http://www.epa.gov/ogc/china/open_environmental.pdf.
[374] Ibid.

will be accountable for their pollution emissions. OEI comes a long way in expanding environmental information disclosure. However, there still remain challenges to its consistent implementation.

Section 4: The Challenges of Implementation

According to Chinese environmental law expert Wang Cangfa, only 10 percent of all environmental laws and regulations in China are actually enforced. [375] There is an explanation for this. The fundamental challenge to nationwide consistent implementation of OEI is due to the very conditions in which economic growth and power authority has been delegated ever since the late 1970s. In political scientist Kenneth Lieberthal's seminal article on China's environmental governance, he traces why decentralization has resulted in a systemic inability to implement consistent environmental protection in China.[376] He reveals that China's economic miracle has been built on a system that has resulted in a decentralizing of political control to foster economic growth. The reasoning behind decentralization was that the Chinese government believed that too strict of central government control was a legacy of the Maoist command economy ideology, which in turn reduced economic incentives and constrained innovation. Therefore, the natural course of action was to decentralize to give local officials wider discretion in finding innovative ways to increase economic growth, especially in rural areas. Lieberthal writes, today's "township and village enterprises have been the most dynamically growing sector of the Chinese economy for more than a decade, providing a substantial portion of

[375] Economy, "The Great Leap Backward," 6.
[376] Kenneth Lieberthal, "China's Governing System and its Impact on Environmental Policy Implementation," *China Environment Series*, Issue 1, 1997, 3-7.

the impetus for the economic miracle."[377] While decentralization has resulted in significant economic advances, China's environment has suffered as a consequence.

The devolving of authority to local rather than central government officials has translated into ineffective environmental protection. Local officials do not prioritize environmental protection because they have no incentive to do so as they are judged by their ability to deliver high economic growth rates. The reasoning here is that if a local official can deliver high rates of economic growth, that same official's chances of being promoted to a higher political rank are dramatically increased. This system of promotion has thus incentivized local officials to become "entrepreneurial." Unfortunately, the most highly profitable companies are also some of the most heavily polluting. A perfect example of local officials prioritizing short-term profitable economic gains was seen in the Dongyang environmental mass incident. Unless local officials are judged by their abilities to balance *both* economic growth and environmental protection, incentives to prioritize environmental protection will be lacking. In addition to the political incentives of local officials, there are also problems regarding the issue of state secrecy.

It was mentioned earlier in Section 3's description of OEI that more specific definitions of what is environmental information and what is not environmental information give local officials less available options to provide excuses for refusing access. While more exact definitions do in fact make that process for local government officials more difficult, these local officials, in theory, still have the ultimate say in defining and categorizing government-held information. Jamie Horsley of Yale Law School says that local officials, under the central government's 1989 State Secrecy Law, have the power to designate environmental information (or any kind of information) a threat to national

[377] Ibid., 5.

security.[378] If a compelling argument is made saying that the disclosure of certain kinds of information would instigate violence or lead to social instability, then that piece of information becomes by definition a "state secret." If information is a state secret, it cannot be disclosed. The discretion of local officials in choosing what information is or is not a state secret creates conflicts of interest. For example, local officials generally will choose to not disclose environmental information on a highly polluting company that at the same time provides employment for thousands of residents.[379] The discretion of local authorities in deeming information a state secret is one of the impediments towards implementing OEI. This discretion is attributed to decentralization.

In her *Foreign Affairs* article, Elizabeth Economy notes that effective market-based fines for polluters are lacking.[380] Often companies have an economic incentive to pollute because pollution fines are lesser than the cost incurred to invest in pollution-reducing technologies or management practices. For example, in 2005 one manager of a coal-fired power plant told Chinese reporters that he was ignoring a government edict requiring all new power plants adopt desulphurization equipment because the cost of adopting technology would be equivalent to fifteen years of pollution fines.[381]

The other challenge towards OEI's implementation is that MEP itself lacks the power and capacity to enforce OEI. Gang He says that local EPBs are not staffed by central government officials

---

[378] Jamie Horsley, "China Adopts First Nationwide Open Government Information Regulations," *freedomonline.org*, May 9, 2007, http://www.freedominfo.org/features/20070509.htm.
[379] Elizabeth Economy, *The River Runs Black: The Environmental Challenge to China's Future* (Cornell University Press, 2004), 92.
[380] Economy, "The Great Leap Backward," 6.
[381] Ibid.

from MEP.[382] Rather, local government officials—because of decentralization—appoint staff to EPBs. This poses a direct conflict of interest, as local officials prioritize economic growth and place environmental protection as secondary. In terms of lacking capacity, a useful analogy is to compare China's MEP with the U.S. Environmental Protection Agency (U.S. EPA).

The U.S. EPA has a staff of over 17,000 employees, not including outside contractors.[383] There are nearly 9,000 in Washington, D.C., alone.[384] China on the other hand barely has 300 professional full-time MEP employees working in the central government's headquarters in Beijing, with only a few hundred scattered throughout the country.[385] Including affiliate agencies and institutions, the total number of personnel delegated responsibility to improving China's environment is at most 2,600.[386] Again, as long as concerns for economic growth continue to be prioritized, environmental protection will always be secondary.

Addressing decentralization is essential to maintaining consistent implementation of OEI throughout China. Until decentralization is addressed, the incentives for local authorities to deviate will be too great, resulting in OEI's inconsistent enforcement.

Conclusion

It was believed by the ancient Chinese people that the rule of emperors was legitimated by the "Mandate of Heaven." The emperor's mandate was predicated on the ability to rule justly, as

---

[382] Gang He, "China's New Ministry of Environmental Protection Begins to Bark, but Still Lacks in Bite," *Earthtrends*, July 17, 2008, http://earthtrends.wri.org/updates/node/321.
[383] Ibid.
[384] Economy, "The Great Leap Backward," 6.
[385] Ibid.
[386] He, "China's New Ministry."

well as preserving social stability. Often preserving social stability translated into maintaining the many agricultural projects that provided sustenance for the Chinese people. Negligence to maintain agriculture and/or widespread natural disasters leading to famine or flooding were signs that Heaven was not pleased with the emperor's rule. If stability could not be maintained, it was perceived that the emperor was out of favor with Heaven, meaning he had lost his mandate. The loss of a mandate meant that the emperor no longer retained legitimacy, justifying a change in government.

Presently, the mandate of the Chinese Communist Party is threatened by growing social instability. If there is anything more terrifying for Chinese leaders today, it is the reality of increasing protests triggered by pollution throughout the country. To preserve their mandate, Chinese leaders have come to the realization that transparency is crucial to solving China's pollution crisis. Transparency has meant that the government has been forced to reduce its control over environmental information. However, there are still many impediments towards implementing full transparency, especially due to the devolution of authority to local officials with the intention of creating economic growth irrespective of environmental concerns.

OEI presents a great opportunity for China's citizenry to force polluters and the corrupt to become accountable for environmental degradation and to change their behavior. Nevertheless, it still remains uncertain whether this new legislation will actually work as intended. Will OEI truly bring about a new paradigm for the *rule of law* in China? Will the corrupt truly be held accountable? In the interim, it is foreseeable that systemic challenges will continue to serve as impediments to justice. But ultimately, only time will tell whether this legislation can truly be an effective mechanism to solving China's pollution problems.

Works Cited

Andrews, Steven. "Seeing Through the Smog: Understanding the Limits of Chinese Air Pollution Reporting." *China Environment Series*. Issue 10, 2008.

Cao, Dong, Genfa Lu, Hua Wang, and Jinnan Wang. *Environmental Information Disclosure: Theory and Practice*. Beijing: Chinese Environmental Science Publisher, 2002.

Dollar, David. "Poverty, inequality and social disparities during China's economic reform." World Bank. 2007. http://www-wds.worldbank.org/external/default/WDSContentServer/IW3P/IB/2007/06/13/000016406_20070613095018/Rendered/PDF/wps4253.pdf.

Economy, Elizabeth. "The Great Leap Backward?" *Foreign Affairs*. September/October, 2007. http://www.foreignaffairs.org/20070901faessay86503/elizabeth-c-economy/the-great-leap-backward.html?mode=print.

----------. *The River Runs Black—The Environmental Challenge to China's Future.* Ithaca: Cornell University Press, 2004.

Freedom House. *Freedom in the World—China*. 2008. http://www.freedomhouse.org/inc/content/pubs/fiw/inc_country_detail.cfm?year=2008&country=7372&pf.

He, Gang. "China's New Ministry of Environmental Protection Begins to Bark, but Still Lacks in Bite." *Earthtrends*. July 17, 2008. http://earthtrends.wri.org/updates/node/321.

----------. “Freedom of Information and Environmental Protection in China.” *Earthtrends*. 2008. http://earthtrends.wri.org/updates/node/324.

Horsley, Jamie. “China Adopts First Nationwide Open Government Information Regulations.” *freedomonline.org*. May 9, 2007. http://www.freedominfo.org/features/20070509.htm.

Kahn, Joseph and Jim Yardley. “As China Roars, Pollution Reaches Deadly Extremes.” *The New York Times*. August 26, 2007. http://www.nytimes.com/2007/08/26/world/asia/26china.html?_r=1&pagewanted=all.

Knickerbocker, Brad. “China now world’s biggest greenhouse gas emitter.” *The Christian Science Monitor*. June 28, 2007. http://www.csmonitor.com/2007/0628/p12s01-wogi.html.

Li, Wanxin. “Opening up the Floor: Environmental Performance Information Disclosure Pilot Programs in Zhenjiang and Hohhot.” *China Environment Series*. Issue 8, 2006.

Lieberthal, Kenneth. “China’s Governing System And Its Impact on Environmental Policy Implementation.” *China Environment Series*. Issue 1, 1997.

Ma, Tianjie. “Environmental Mass Incidents in Rural China: Examining Large-Scale Unrest in Dongyang, Zhejiang.” *China Environment Series.* Issue 10, 2008.

Ministry of Environmental Protection. *Official Report on China’s Environment.* (in Chinese). 2007. http://www.chinaenvironment.com/uploads/454/2008-8-25/1.pdf.

Moore, Allison and Adria Warren. “Legal Advocacy in Environmental Public Participation in China: Raising the Stakes and Strengthening Stakeholders.” *China Environment Series*. Issue 8, 2006.

Mrasek, Volker. “China’s Greenhouse Gas Emissions Threaten to Double.” *Spiegel Online Internationl*. March 6, 2009. http://www.spiegel.de/international/world/0,1518,611818,00.html.

Organization for Economic Co-Ordination and Development. *OECD*
Environmental Performance Reviews: China. Volume 24. 2007.

Rosenthal, Elisabeth. “China Officially Lifts Filter on Staggering Air Pollution Data.” *The New York Times*. June 14, 1998. http://www.nytimes.com/1998/06/14/world/china-officially-lifts-filter-on-staggering-pollution-data.html.

State Environmental Protection Administration of China. *Measures on Open Environmental Information (for Trial Implementation)*. 2007. http://www.epa.gov/ogc/china/open_environmental.pdf.

US Embassy-China. “The Fading of Chinese Environmental Secrecy.” *US Embassy-China webpage*. 1998. http://www.usembassychina.org.cn/english/sandt/chplca/htm.

World Bank. *Cost of Pollution in China: Economic Estimates of Physical Damages*. 2007. http://siteresources.worldbank.org/INTEAPREGTOPENVIRONMENT/Resources/China_Cost_of_Pollution.pdf.

Zhang, Ke. “Group monitors China’s water polluters using online mapping.” World Watch Institute. September 26, 2006. http://www.worldwatch.org/node/4622.