ALL-STAR
Invitational MUN Conference
China 2021

2021.05.02-05.04 | Shanghai

Commission on Crime Prevention and Criminal Justice (CCPCJ)

#BACKGROUND GUIDE

Commission on Crime Prevention and Criminal Justice

Topic A: Cybercrime

Topic B: The Role of Secrecy in Crime Prevention and Criminal Justice

Committee History

The CCPCJ is the Commission on Crime Prevention and Criminal Justice. The organization was established by the Economic and Social Council in 1992 at the request of the United Nations General Assembly. The CCPCJ serves as a policymaking body within the UN aimed at improving international actions to combat national and international crime and ensuring the efficacy and fairness of criminal justice administration systems. The organization also aims to build peace and security by serving as an international forum that allows nations across the globe to come together to share strategies and identify priorities regarding crime prevention. In addition to maintaining its own functions within the UN, the CCPCJ is the preparatory body to the United Nations Crime Congresses, and serves as a governing body of the United Nations Office on Drugs and Crime. The CCPCJ works with other UN bodies that have mandates in crime prevention and criminal justice, working to pass resolutions and formulate concrete solutions to ensure that the fundamental principles of crime prevention and justice continue to be upheld around the world.[1]

1 "The Commission on Crime Prevention and Criminal Justice," accessed November 13, 2018, http://www.unodc.org/unodc/en/commissions/CCPCJ/index.html.

TOPIC A: CYBERCRIME

Statement of the Problem

An Introduction to Cybercrime: A Case Study of Stuxnet

In 2010, the government of Iran had a problem.

Two related problems, to be precise. The first was that it had nuclear enrichment facilities it was trying to keep secret. It could not allow the rest of the world to know that it was trying to build a nuclear weapon. The second was that the centrifuges that were meant to enrich uranium in these facilities were failing. The motors in the centrifuges kept tearing themselves apart, and replacing the broken parts did not solve the problem. No Iranian scientist could figure out what was going on.[2]

Finally, a German cybersecurity expert named Ralph Langner realized what was happening. Shockingly, an extremely sophisticated computer system infection was slyly changing the speeds of the centrifuges in the machines and providing false feedback to the people overseeing the devices so that they would have no clue as to what was going wrong. As a result, the people in charge thought that the centrifuges' faultiness stemmed from bad parts, even though that was not true.

Even more shockingly, it was revealed that the **malware** (malicious software), known as Stuxnet, had not been sponsored by some independent or rogue hacker, but by none other than the United States government in collaboration with Mossad, Israel's intelligence agency.[3] The operation that they had worked on together was codenamed "Olympic Games" and was only a component of a larger project: it complemented a simultaneous effort, led by Israeli agents, to assassinate Iranian scientists.[4]

On the surface, it's difficult to see why the Stuxnet hack, while fascinating, matters so much. Yet it is so crucial that one cybersecurity expert, Adam Segal of the Council on Foreign Relations, an American think-tank, considers the year that Stuxnet occurred to be the, "Year Zero in the battle over cyberspace."[5] Segal concedes that large data breaches and cyberattacks had

2 Adam Segal, *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age*, 2nd ed. (New York, NY: Public Affairs, 2017), 1.
3 Ellen Nakashima and Joby Warrick, "Stuxnet was work of U.S. and Israeli experts, officials say," *The Washington Post*, June 2, 2012, accessed November 10, 2018, https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html?utm_term=.d72a98a491a4.
4 Segal 2.
5 Segal 1.

happened in the past, but Stuxnet was special since it helped to kill off the idea that cyberspace was, "a digital utopia, free of geopolitics."[6] It also made it clear that a major world power was committed to developing offensive cyber capabilities. Furthermore, Stuxnet may have led to critical developments in diplomacy: it may have persuaded Iran to be more open to negotiation, and convinced it to agree to a deal on its nuclear program in 2015.[7]

To put it differently, Stuxnet was so important and unprecedented because it challenged a world order that had existed since 1648, when the Peace of Westphalia was reached and the modern nation-state was formed. The Westphalian order was one where each nation had a monopoly of legitimate force within its borders, and one where no one else could challenge a nation's domestic authority.[8] Stuxnet flipped that concept on its head; It was the first time a cybercrime influenced international politics on such a grand scale.

Introduction to the Problem of Cybercrime

The CCPCJ targets the most urgent problems in national and transnational crime, and few problems are more troubling to the world order than cybercrime. However, even though cybercrime is one of the most complex issues our world faces today, a widely accepted standard definition of the concept remains elusive. In fact, according to the United Nations Office on Drugs and Crime, there does not exist a concrete international definition of cybercrime.[9] However, many efforts have been made in the past to discuss what categories of cybercrime exist. The Global Programme on Cybercrime notes that there are two broad categories that most, if not all, cyber crimes fall into: **cyber-dependent cybercrime**, and **cyber-enabling cybercrime**. These categories are utilized by various law enforcement agencies around the world, like the Crown Prosecution Service in the United Kingdom, to better categorize cybercrimes.[10]

Cyber-dependent cybercrimes are crimes that can only be committed through the use of **information and communications technology** (**ICT**). Examples of ICT include telephone and computer networks; more generally, all modern technology that allows for interaction between people and organizations is considered ICT.[11] Some examples of cyber-dependent cybercrimes would be the creation of malware with the goal of disrupting network activity or deleting data stored in a system, or hacking a computer in order to steal data from it.

6 Ibid.
7 Segal 3.
8 P. W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (New York, NY: Oxford University Press, 2014), 193.
9 United Nations, "Global Programme on Cybercrime," United Nations Office on Drugs and Crime, accessed July 9, 2018, https://www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html.
10 Crown Prosecution Service, "Cybercrime - Prosecution Guidance," CPS Prosecution Guidance, accessed July 9, 2018, https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance.
11 Margaret Rouse, "ICT (Information and Communications Technology, or Technologies)," TechTarget, accessed July 9, 2018, https://searchcio.techtarget.com/definition/ICT-information-and-communications-technology-or-technologies.

Cyber-enabled cybercrimes are crimes that would be able to be committed without the use of ICT, but whose scope and scale can be broadened with the use of ICT. Cyber-enabled cybercrimes tend to be more traditional crimes. For example, the sale of illicit drugs can be achieved in person and without a computer network, but a computer network allows a seller to reach a greater number of interested purchasers and organize their market in a more efficient manner. Other examples of cyber-enabled crimes include cyberbullying, cyber-enabled fraud, or cyber counterfeiting or forgery.

Causes of Cybercrime

The most immediate and evident cause of cybercrime is the simple fact that it pays off: cybercriminals who want to extort money are able to do so simply using technology, and cybercriminals who want to steal information from a database are able to gain information easily. Cybercrime is enabled by lax security in computer systems and networks. For example, imperfections in computer software may make it possible for hackers to read sensitive information such as a computer's memory and passwords.[12] Cybercrime is also enabled by the fact that it can be committed from any physical location, as long as the user has a computer linked to the network. This remoteness allows cybercrimes to be committed at more times and locations than standard crimes can be.

Another cause of cybercrime is the sense of accomplishment that a successful cybercrime affords its doer. The Federal Bureau of Investigation of the United States considers, "computer geeks looking for bragging rights," a cause of cybercrime, and research has shown that teenagers are particularly susceptible to being motivated to start committing cyber crimes, not only for bragging rights, but also because of peer pressure.[13] A recent study by the UK's National Crime Agency found that a number of teenagers who would not likely engage in traditional crime are instead engaging in cybercrime.[14] Young people who commit cybercrimes are often driven not by a financial motive, but rather a desire to be "cool."

Finally, the lack of legal consequences for cybercriminals who are caught facilitates the occurrence of crime. Only 72% of countries in the world have some cybercrime legislation in place, and more than 30 countries have no cybercrime legislation in place at all.[15] Moreover, when the identity of a cybercriminal is discovered, it may be unclear as to which law enforcement agency has the authority to arrest them. For instance, if the cybercrime committed involves victims from multiple countries, the law enforcement agencies from those countries may be

12 Douglas Busvine and Stephen Nellis, "Security Flaws Put Virtually All Phones, Computers at Risk," Reuters, https://www.reuters.com/article/us-cyber-intel/security-flaws-put-virtually-all-phones-computers-at-risk-idUSKBN1ES1BO.
13 FBI, "Cyber Crime," What We Investigate, accessed July 9, 2018, https://www.fbi.gov/investigate/cyber.
14 National Crime Agency, "Pathways into Cyber Crime," NCA Intelligence Assesment, last modified January 13, 2017, accessed July 9, 2018, http://www.nationalcrimeagency.gov.uk/publications/791-pathways-into-cyber-crime/file.
15 United Nations, "Cybercrime Legislation Worldwide," United Nations Conference on Trade and Development, accessed July 9, 2018, http://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Cybercrime-Laws.aspx.

reluctant to cooperate with each other. In addition, a cybercrime's country of origin may be difficult to ascertain, which also makes it difficult to prosecute cybercriminals.

Overall, the current return on investment in cybercrime is high, and the risk is low. This increases the motivation for cybercriminals to commit cybercrime, especially since the development of legal penalties for cybercrimes tends to lag behind the development of new types of cybercrime.

Effects of Cybercrime

Cybercrime deals economic harm to governments, individuals, and the world at large. In 2016, $600 billion – close to one percent of the world's total GDP – was lost to cybercrime, a large increase from the $445 billion lost in 2014.[16] More than half of all businesses in the United Kingdom were the victim of a cybercrime in 2016.[17] Cybercriminals mostly target larger businesses since they are more valuable targets, but cybercrime has also forced small businesses to make costly investments in cybersecurity, as a single well-organized attack can potentially completely destroy their infrastructure.

Cybercrime also deals emotional harm to individuals who may be the victims of online bullying or harassment. Nearly a sixth of all high schoolers in the United States were bullied electronically in 2015.[18] Furthermore, cyberbullying has been linked to increased rates of depression in teenagers, demonstrating its exacerbation of in-person bullying.[19]

16 James Andrew Lewis, "Economic Impact of Cybercrime," Center for Strategic & International Studies, last modified February 21, 2018, accessed July 9, 2018, https://www.csis.org/analysis/economic-impact-cybercrime.

17 Rachael White, "Cyber Security Breaches Cost British Businesses Almost £30 Billion in 2016," Beaming, last modified March 1, 2017, accessed July 9, 2018, https://www.beaming.co.uk/press-releases/cyber-security-breaches-cost-businesses-30-billion/.

18 CDC, "Trends in the Prevalence of Behaviors That Contribute to Violence," Youth Risk Behavior Survey, https://www.cdc.gov/healthyyouth/data/yrbs/pdf/trends/2015_us_violence_trend_yrbs.pdf.

19 Stephanie Pappas, "Cyberbullying on Social Media Linked to Teen Depression," LiveScience, last modified June 22, 2015, accessed July 9, 2018, https://www.livescience.com/51294-cyberbullying-social-media-teen-depression.html.

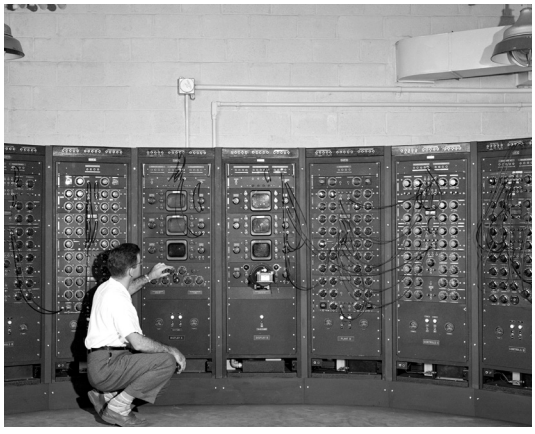
A History of the Problem

The history of cybercrime can be divided into four stages: the stage of germination, the stage of rapid development, the stage of rapid expansion, and the stage of routinization.[20] During all four of these stages, law enforcement around the globe has always lagged behind the cybercriminal acts themselves.

The **stage of germination** began from the late 1940s and lasted through the late 1960s.[21] A defining feature of this stage is that there was a very small "market" for computers in this early stage: because computers were expensive and rare at the time, people needed to share the use of computers in order to afford them. As a result, the line between unauthorized use of computers and authorized use of computers at this time was very blurred, with many people possessing access to the same device.

The stage of germination was also characterized by legislatures not providing any specific countermeasures against the phenomenon of cybercrime.[22] A principle of "*nullum crimen, nulla poena sine lege*," (Latin for "no crime without law, no punishment without law") was established to prevent perpetrators' fundamental rights from being violated. The exception to this hands-off approach to fighting cybercrime was when it came to phone systems violations. While the U.S. government had not yet figured out how to enact laws against computer systems-based crimes, phreakers (an early form of hacker) had previously intruded into and interfered with telecommunications systems, snagging free long-distance phone calls in the process. Because phone systems had been threatened, the U.S. took action to prevent tampering with phone systems.[23] Overall, because there were mostly no laws specifically targeting cybercrime, little could be done to deter cybercriminals. Some deterrence was achieved through exploiting existing laws, but not enough.

One factor preventing cybercrime from being as widespread as it could have been during the stage of germination was that the internet was not open to general users.[24] The internet began in the mid-1960s as a program of the U.S. Department of Defense, and at the time, it was only primarily connected to various government institutions.



20 Johannes Xingan Li, "Cyber Crime and Legal Countermeasures: A Historical Analysis," *International Journal of Criminal Justice Sciences* 12, no. 2 (July-December 2017): 197.
21 Ibid.
22 Ibid., 198.
23 Ibid.
24 Ibid.

When the stage of germination began, the first computers had just been invented. When the stage of germination ended, the general public had begun to pay more attention to computers and expanded market for computers. To put that into perspective: there were 400 computer installations in the U.S. at the beginning of the 1950s, in the middle of the stage of germination. By the end of the 1960s, and the end of the stage of germination, that number had risen to 60,000.[25]

The **stage of rapid development** began in the 1970s and lasted until the end of the 1980s. During this stage, individuals and organizations started to depend on computers more, and computer manufacturers paid more attention to the design of a computer: it gradually changed from a bulky thing to a more beautiful, user-friendly machine. As distinguished professor of communications and society Vincent Mosco put it, "The computer would be growing in power while withdrawing as a presence."[26]

As the stage of rapid development progressed, the previously blurred line between unauthorized and authorized use of a system became more clear. This is because as time went on, more computers were available on the market for users to obtain. Whereas one may have needed to previously share a computer with others, now one could have a computer all to themselves. Intruding into other people's systems could clearly be labeled "abuse" when you could very well use your own system.[27] As a result, during the stage of rapid development, cybercrimes fell into five key categories: cyber vandalism, theft of information, theft of services, theft of property, and fraud.[28]

The 1980s were a time of many "firsts" in the field of cybercrime: in 1984, the term "cyberspace" was first used in a fictional work by William Gibson, a science-fiction writer.[29] Disturbingly, murdering someone with a computer became realistic for the first time in this period; In 1982, a group of hackers intruded into a system where they could change the medical records of cancer patients.[30] In 1983, the first computer virus was written by Fred Cohen, a graduate student at the University of Southern California.[31] The first virus infection was then recorded in 1986.[32]

In the early 1970s, most developed countries introduced laws criminalizing computer crime, and in the 1980s, more laws and regulations were implemented. Curiously, Nordic countries led the charge on this matter: all of them had data-protection laws in place during this period.[33]

25 Ibid., 197.
26 Mosco, 2004.
27 Li, 199.
28 Ibid.
29 Li, 200.
30 Ibid.
31 Overill, 102.
32 Ibid.
33 Li, 201.

Overall, during the stage of rapid development, the rate of cybercrime grew. While the costs of it were increasing due to increasing law enforcement, the costs of cyber crime were lower than other well-punished crimes.

The **stage of rapid expansion** consisted of the whole of the 1990s. During this stage, relevant legislation began to be broadly implemented by politicians who tied computer communication to economic growth, democracy, and a better environment. This change happened in part because the World Wide Web (WWW) was invented, and the internet was no longer limited to academic and official uses.[34] With the WWW, the internet became globalized and available to average users.

During this period, new incentives arose for perpetrators of cyber crimes. With more ordinary people using the internet, there was more personal information available on the internet to be stolen. Taking advantage of the increased number of computer users, cyber criminals began to abuse electronic communications by sending large-scale unsolicited e-mails known as spam. Moreover, copyright piracy became a problem at this stage, with users setting up unregulated websites where pirated audio, video, and text works could be exchanged.

In response to these new forms of cyber crime, antivirus businesses and companies started developing. By 1990, many antivirus products were developed and introduced to the market.

During the stage of rapid expansion, web sites became targets for attacks, and the rate of attacks on them increased at a startling rate: in 1998, 72 websites were defaced by 47 attackers, but in the very next year, 1,079 web sites were defaced by 430 attackers.[35] Similarly, in 1998, the FBI opened 547 cases of "computer intrusion," but in 1999, that number grew to 1,154.[36]

Despite these numbers, overall, cybercrime had reached a stage of saturation, where its growth rate was decreasing.[37] Because more users were connected through more networks, cybercriminals became easier to trace. In addition, the punishment for committing cyber crimes became more severe.

In particular, 1990, the starting year of the stage of rapid expansion, was an "unprecedented and startling year for the growing world of computerized communications."[38] This was because the power of law enforcement was on full display: "there came a nationwide crackdown on illicit computer hackers, with arrests, criminal charges, one dramatic show trial, several guilty pleas, and huge confiscations of data and equipment all over the United States." 1990 was also an

34 Ibid., 202.
35 Ibid.
36 Ibid.
37 Ibid., 203.
38 Sterling, xiii.

important year for cybercrime in the UK, as the Computer Misuse Act of 1990 was passed into law.[39]

The **stage of routinization** spans the period of time from the early 2000s to today. In this era, cybercriminals have become more innovative than ever, as large-scale Denial of Service attacks have taken place against many web sites and financial institutions, including SunTrust, JPMorgan Chase, Wells Fargo, and HSBC.[40] These attacks, in which, "hackers use thousands of computers or servers to flood a website with so much data that it can no longer respond," caused great panic in society about the infrastructure of the internet.[41] [42]

Common cybercrime tropes started to appear in the stage of routinization. The advance-fee fraud, technically termed the 419 fraud (after a section of the Nigerian legal code), and better known as the "Nigerian prince" scam, began to appear. In this scam, the scammer poses as a figure of importance who promises the victim a large sum of payment, but not before requiring a small up-front payment from the victim. After the victim transfers money voluntarily to the criminal, the scammer does not follow up on the offer. On average, Nigerian prince scam victims have lost around 5,575 dollars in the course of the scam.[43]

The overall negative financial impact of cybercrime is significant but decreasing, according to yearly surveys conducted by the Computer Systems Institute and the FBI.[44] In 2003, 530 survey respondents' losses totaled 201.7 million dollars; in 2004, 494 respondents lost 141.5 million dollars, and in 2005, 639 respondents lost 130.1 million.

On July 1, 2004, the Convention on Cybercrime, the first international treaty addressing internet and computer crime, took effect. 57 parties have signed the treaty so far, and it looks to be an important bedrock for countries to tackle the upcoming challenges that await.

39 Overill, 102.
40 Segal, 5.
41 Ibid.
42 Li, 203.
43 Ibid.
44 Ibid.

A Past Actions

International Treaties

The Council of Europe's Convention on Cybercrime, 2001

The Council of Europe's 2001 Convention on Cybercrime, or the Budapest Convention, was the first international treaty to address cybercrime. It is a binding agreement that has been ratified by 57 states, most of which are European and Western countries.[45]

The states who ratify the convention agree to adopt legislation appropriate to their countries that combat a wide array of offenses, such as: illegal access of a computer, illegal interception, data interference, computer-related fraud, offenses related to child pornography, and offenses related to copyright matters.[46]

While the convention covers a wide array of topics, it is still not all-encompassing. An Additional Protocol to the Convention on Cybercrime entered into force in 2006. The Additional Protocol requires participating countries to criminalize cyber acts that are racist or xenophobic in nature.[47]

However, many important countries have refused to sign the Convention, much less its Additional Protocol. Russia has refused to sign the Convention, stating that doing so would violate its national sovereignty. In particular, Russia took particular offense at Article 32 of the Convention, which grants a country transborder access to publicly stored data.[48] [49] Other important countries, like India, have also not signed on to the Convention, citing concerns about sharing pieces of private information with foreign law enforcement agencies.[50]

The 2012 International Telecommunications Union Agreement

At its 2012 meeting in Dubai, the International Telecommunications Union (ITU) passed a controversial agreement.

When the ITU was founded in 1865, its name was the International Telegraph Union, and its founders agreed that it would regulate correspondence by safeguarding the right of privacy for all materials, implementing standard international tariffs, and deciding on the international

45 "Chart of signatures and ratifications of Treaty 185," Council of Europe, last modified October 11, 2018, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures.
46 "Convention on Cybercrime," Council of Europe, last modified November 23, 2001, http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf.
47 "Details of Treaty No.189," Council of Europe, last modified January 28, 2003, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189.
48 Keir Giles, "Russia's Public Stance on Cyberspace Issues," last modified 2012, https://ccdcoe.org/publications/2012proceedings/2_1_Giles_RussiasPublicStanceOnCyberInformationWarfare.pdf.
49 "Convention on Cybercrime," Council of Europe.
50 Rahul Tripathi, "Home Ministry pitches for Budapest Convention on cyber security," The Indian Express, last modified January 18, 2018, https://indianexpress.com/article/india/home-ministry-pitches-for-budapest-convention-on-cyber-security-rajnath-singh-5029314/.

standard of Morse code, among other methods. Over time, the ITU's role expanded to regulating messages not just sent over telegrams, but also sent over telephones and radios as well.[51]

In 2012, a meeting was called to determine whether the ITU's role should expand even further, to include ensuring governments had sweeping powers, including the right to ensure its people had the right to get to a webpage. Interestingly enough, Western democratic countries like the UK and US did not like this proposal, as giving national governments control over the internet would also mean giving them the right to ensure that people who wanted to access certain web pages couldn't get there. These democratic countries believed that fears about cybersecurity were being used by other countries to encroach on international internet freedoms.[52] Meanwhile, the countries who were advocating for the proposal were countries like Russia, China, and Sudan, who wanted to regain sovereignty over their parts of the internet.[53]

The vote to accept the proposal ended up passing. However, though a large number of states have expressed support for the ITU's treaty, not enough states have ratified it yet for it to become binding. With so many important states opposing the treaty, it is unclear if it will ever be ratified or enforced, and it is unclear if the ITU will ever regain the esteem it had as an organization.[54] [55]

How can we write effective treaties in the future?

The thinker Martha Finnemore suggested that countries ought to cooperate using a strategy she terms "grafting."[56] A reference to a gardening technique, "grafting" means that countries should build off of old frameworks and roots rather than try to plant the seeds for a new framework. With that in mind, delegates should keep in mind the existing international legislation when proposing solutions to the problem of cybercrime.

Both the Convention on Cybercrime and the ITU Treaty do something particularly well: they make a point of going after "double crimes"—cyber actions that two nations already recognize as illegal.[57] Treaties can also be effective if they encourage countries to use already existing, more mundane laws to go after cyber criminals while those countries develop more complex cyber crime laws to catch up with the times.[58] A famous example of a government using mundane laws to go after a non-mundane criminal would be the example of how American prosecutors were able to put Al Capone in jail. Capone was convicted of tax fraud, something that was easier to prove his guilt in, rather than a more serious charge like murder. Similarly, countries can try

51 Singer and Friedman, 183.
52 Ibid., 184.
53 Ibid., 184.
54 Ibid., 183.
55 A digital cold war?," The Economist, last modified December 14, 2012, https://www.economist.com/babbage/2012/12/14/a-digital-cold-war.
56 Singer and Friedman, 187.
57 Singer and Friedman, 180.
58 Singer and Friedman, 207.

to use already existing laws against money laundering to prosecute cyber criminals who shadily dabble in digital currencies rather than attempt to craft a new law for each new kind of financial cybercrime that arises.[59]

Moreover, some cybersecurity thinkers have suggested cybercrimes can be better combated if all countries to agree to take responsibility for any attacks that emanated from within their own borders.[60] However, while that sounds like a simple thing to agree to, it is important to remember that state-supported cyber attacks, like Stuxnet, exist.

59 Singer and Friedman, 207.
60 Singer and Friedman, 179.

A Possible Solutions

Changing the Cultural Norms Surrounding Cybersecurity (or, what we can learn from the CDC)

Strange as it may sound, many hints of possible solutions to the problem of cybercrime can be gleaned by looking at how the problems of global health are currently being combatted.

P.W. Singer and Allan Friedman, two fellows at the Brookings Institution, write in their book about cybersecurity that the field can learn much from the creation of the Centers for Disease Control (CDC), which they call, "one of the most successful government agencies in history."[61] The CDC managed to foster collaboration among individuals, private companies, and nations in order to not only prevent "deliberate attacks" (like biological weapons attacks) from occurring but also to change the culture around preventing their root causes.[62]

Singer and Friedman argue that the cybersecurity community ought to take a page from the CDC's playbook. They suggest the cybersecurity community pay attention to two strategies in particular. Firstly, they advocate for incentives for companies to practice good cybersecurity habits as well as cooperate with each other. Secondly, they believe in building a culture where each actor feels an individual obligation to behave responsibly when it comes to cybersecurity.

Incentives for Cybersecurity

In thinking about possible solutions to the problem of cybercrime, it is worth revisiting why cybercrimes occur in the first place.

Cybercriminals are often able to hack companies because a company's cyberdefenses are poor. However, the company itself is often to blame for that: several American companies willingly refuse to upgrade their cyber systems.[63] Why? Because companies find it a waste of precious time to invest in cyberdefense resources whose benefits cannot be easily quantified like most other profits can. Though investing in cyberdefense resources is the smart choice for companies when it comes to the long-term, many companies find it very difficult to prioritize that over their short-term goals.[64]

Thus, some cybersecurity experts have suggested that governments ought to develop basic standards of cybersecurity that companies and individuals are required to comply with, just as buildings are required to comply with safety and fire codes.[65] Indeed, the SANS Institute

61 Singer and Friedman, 173.
62 Ibid.
63 Singer and Friedman, 209.
64 Ibid.
65 Singer and Friedman, 220.

previously published a list of the Top 20 Critical Security Controls that could be used as a starting point for this purpose. One study showed that the good that could result from enforcing the Top 20 Controls was not to be underestimated: if companies were to follow them, up to 94 percent of all security risks would be stopped.[66]

Meanwhile, companies refusing to be transparent with their customers after a breach of security has occurred makes for another example of companies prioritizing their short-term incentives over long-term incentives. A company who admits that its security was compromised will likely receive backlash and lose customers' trust in the short-term. However, in the long-term, the company creates accountability for itself and also signals a gradual change of norms to other companies in the field.[67] In this case, as with the matter of basic standards of cybersecurity, governments ought to mandate a baseline level of transparency from companies regarding cyberattacks. Some have suggested that companies who are transparent enough ought to be economically sanctioned.[68]

Another reason why cyberattacks are so damaging to companies is because many companies hoard resources to their financial advantage, and refuse to share information with each other. For example, banks sometimes hire private firms to determine if their brand is being used to create **phishing websites**, which are websites that attempt to fraudulently obtain people's sensitive information. Those firms then undergo a process of taking the misleading websites down. But a study recently revealed that while two different takedown companies each discovered websites for the other's clients, they had no incentive to remove them. As a result, the companies and banks wasted an estimated $330 million.[69] This problem could be tackled by encouraging more firms and banks to share information with each other.

As Singer and Friedman point out, just like the CDC encourages hospitals, universities, and research centers to share their discoveries with each other, a "cyber CDC" could encourage private companies, government institutions, and research centers to share anti-cybercrime strategies and information with each other.[70]

Building an ethic of individual responsibility

The CDC has encouraged individuals to adopt responsible behaviors when it comes to preventing the spread of disease. For example, the CDC recommends that people take the time to wash their hands to prevent the spread of the flu.[71]

66 Singer and Friedman, 221.
67 Singer and Friedman, 228-9.
68 Zachary K. Goldman, "Sanctioning Cyber Crime: The New Face of Deterrence," Council on Foreign Relations, last modified May 19, 2015, https://www.cfr.org/blog/sanctioning-cyber-crime-new-face-deterrence.
69 Singer and Friedman, 222.
70 Singer and Friedman, 175.
71 Singer and Friedman, 176.

Similarly, individuals ought to adopt responsible behaviors and practice "cyber hygiene" when it comes to computer-related activities. After all, individuals who are negligent in their cyber activities can be considered to be behaving much in the manner that individuals who refuse to get vaccinated behave: they compromise not only themselves, but also other people who may use the individual's computer, or if other people are on the same network.[72]

Individuals ought to use strong and different passwords for all their online accounts, take advantage of multifactor authentication, and update their antivirus software frequently.[73] In addition, some have suggested that governments ought to launch awareness campaigns about the importance of staying secure on the web, and that "cyber hygiene" ought to be made a cornerstone of the curriculum taught in schools. The US government has launched a public awareness campaign titled "Stop.Think.Connect." and has also designated a National Cyber Security Awareness Month, but further actions can be taken on the issue.[74]

There is yet another parallel with the CDC to be drawn here when it comes to the question of education: if you have a question about how to protect yourself from the common cold or the newest strain of the flu, you can go to the CDC's website for advice on how to do so.[75] Thus, Singer and Friedman favor the creation of a "Cyber CDC" that can manage a "one-stop shop" website for users who have questions on how to troubleshoot specific cybersecurity issues.

"Red Teams" and "Hack Backs" (or, how hackers can actually help stop cybercrime)

Red Teams

On Halloween morning of 2012, some Facebook employees received a startling message. It was an email from an FBI agent who frequently briefed them on security matters. The email alerted security engineers to the fact that an unknown entity had published code to Facebook's site and had access to the "live build" that runs the website. The IP address associated with the entity suggested that the code was published from Beijing.

The email threw many workers into a panic, as many engineers wondered how such a hack could have happened. Luckily, a group of workers was able to find a method to remove the malicious code from Facebook's servers and find the source of the threat. Even more luckily for them, and for Facebook, the cyberattack wasn't real.[76]

72 Singer and Friedman, 176-7.
73 Singer and Friedman, 243-5.
74 "STOP. THINK. CONNECT. ™," U.S. Department of Homeland Security, last modified September 26, 2018, https://www.dhs.gov/stopthinkconnect.
75 Singer and Friedman, 174.
76 Dan Goodin, "At Facebook, zero-day exploits, backdoor code bring war games drill to life," Ars Technica, last modified February 10, 2013, https://arstechnica.com/information-technology/2013/02/at-facebook-zero-day-exploits-backdoor-code-bring-war-games-drill-to-life/.

To be clear: the cyberattack had absolutely happened, but it was not coming from foreign hackers. Rather, Facebook had hired a group of independent cybersecurity professionals to hack into Facebook's system as a drill and so fooled workers into thinking the attack was coming from somewhere that seemed far more sinister.

The "hackers" had spotted a zero day vulnerability in Facebook's security, and took advantage of it. Zero days are previously unknown vulnerabilities in software. They are named as such because once a hacker takes advantage of one, the software developer has zero days to respond to the problem.[77] Zero days are so feared that some websites have started to offer money to skilled individuals who can alert them to bugs in their system, resulting in a program known as bug bounty hunting.[78]

The professionals that were hired by Facebook to hack into Facebook were known as a "**red team.**" The term comes from the military, where a "red team" attacks a "blue team" to test whether the latter can withstand the force of the attack.[79] Red teams are people, usually outside contractors, who are hired by a company to test how secure a company's defenses are. Ryan McGeehan, Facebook's former security director, summed red teams up as follows: "When you can't find the bad guys, make some up."[80]

Hiring skilled security specialists to find bugs in software is undoubtedly expensive,[81] but the advantages of red team drills are numerous. First and foremost, like a military war game, a red team simulation gives a tech company's workers a chance to see how they would respond in a stressful situation. Employees can plan for the worst all they want, but it is one thing to have a plan and another to truly be able to act on it in a high-pressure situation.[82]

Secondly, red teams can point out unfixed vulnerabilities within a company's system. Post-crisis drill, security experts can take the time to figure out what went wrong and develop solutions to

77 Segal, 3.
78 Nick Jenkins, "The Hitchhiker's Guide to Bug Bounty Hunting Throughout the Galaxy.," Medium, last modified January 30, 2018, https://medium.com/@Nick_Jenkins/the-hitchhikers-guide-to-bug-bounty-hunting-throughout-the-galaxy-474ddb87ae15.
79 Doug Drinkwater and Kacy Zurkus, "Red team versus blue team: How to run an effective simulation," CSO, last modified July 26, 2017, https://www.csoonline.com/article/2122440/disaster-recovery/emergency-preparedness-red-team-versus-blue-team-how-to-run-an-effective-simulation.html.
80 Ryan McGeehan, "Red Teams," Medium, last modified March 30, 2015, https://medium.com/starting-up-security/red-teams-6faa8d95f602.
81 Goodin, "At Facebook," Ars Technica.
82 Singer and Friedman, 211-2.

fix the vulnerabilities. To put it differently, a strong cyber offense can improve a strong cyber defense.[83]

Thirdly, red teams can foster a sense of cooperation between workers in different departments at a company. Lawyers and managers likely will approach a crisis differently than cybersecurity professionals woud. A red team simulation forces employees from all across a company to develop effective methods of communication with each other.[84]

The use of red teams can benefit not just private companies, but national governments as well. Think tanks in Washington, DC and Beijing have hosted cyber simulations of hacks with representatives from the American and Chinese governments.[85] Thus, red teams can help to warm icy diplomatic relations between countries, if ever so slightly.

Facebook's use of red teams ended up paying off. A few months after the security drill, a real hacker infiltrated several engineers' computers. The attack was thwarted, and no major damage was done.[86]

Hack Backs, and the advantages and disadvantages of legalizing them

There are several other examples of how intentional hacking can benefit the victims of a cybercrime. For instance, Shawn Carpenter was a security analyst at Sandia National Laboratories who was recruited to investigate a possible hack. Computers at Lockheed Martin, a defense contractor who managed Sandia, had started to suddenly crash. By looking at the malware (malicious software) in Lockheed Martin's system, Carpenter and the other members of his team were able to determine that the intruders were likely hacking in from China. They erased the malware from Lockheed Martin's computers, and the investigation was considered to be finished.[87]

However, Carpenter was not yet satisfied with what he and his team had achieved. He wanted to know more about the hackers' intentions, so he built a trap for them by creating "honeypots"—caches of documents that trick hackers into thinking they've successfully hacked into the system they wanted to when they've actually just hacked into a replica decoy.

Eventually, Carpenter was able to trace the hackers' activity to a server in South Korea, break into that server, and determine exactly what information had been stolen from Lockheed Martin. In this way, Carpenter was able to warn people at Lockheed Martin that military blueprints sensitive

83 Singer and Friedman, 215.
84 Singer and Friedman, 215-6.
85 Singer and Friedman, 214-5.
86 Singer and Friedman, 211.
87 Nicholas Schmidle, "The Digital Vigilantes Who Hack Back," The New Yorker, last modified May 7, 2018, https://www.newyorker.com/magazine/2018/05/07/the-digital-vigilantes-who-hack-back.

to US national security had been stolen by foreigners. But despite his good intentions, he was fired from his job for being "insubordinate" and in "violation of the law," although he later won a lawsuit against his former employer.[88]

What Carpenter did is known to the cybersecurity community as a "hack back." Hack backs occur when firms or individuals that have been hacked go after their attackers' own computers. They are sometimes equated with vigilantism.[89] Hack backs are currently prohibited in some countries, like the US, whose 1986 Computer Fraud and Abuse Act makes it illegal for anyone to "knowingly" access a computer "without authorization." Violating the Act can lead to a prison sentence of up to twenty years.[90]

Counterparts to the Computer Fraud and Abuse Act exist in a few countries. For example, the UK's Computer Misuse Act of 1990 introduced the offense of "unauthorised computer access" into law.[91] In some other countries, the legality of hack backs is more dubious.[92]

Some voices within the cybersecurity community are calling for a revamping of laws so that computer users who hack back are shielded from prosecution. (Recently, a US Congressman introduced a bill "to provide a defense to prosecution…for persons defending against unauthorized intrusions into their computers.")[93]

There are a number of advantages to legalizing hack backs. One of the foremost advantages of allowing individuals or private companies to hack back is that it may allow them to determine who committed the original hack and how much damage was done by it much quicker than an under-resourced, over-burdened law enforcement agency like the FBI could.[94] If it seems surprising that law enforcement agencies could be overburdened, it is important to keep in mind it's estimated that ninety percent of American companies have been hacked.[95] Moreover, private firms and individuals often have technical expertise that government agencies do not.[96]

Hack backs can also help to mitigate the damage done to companies. A successful hack back might allow a company to determine what information has been stolen from it. In Carpenter's case, he was able to determine exactly which military blueprints' secrets had been compromised; meanwhile, in the case of a credit card company, a hack back might allow them to determine

88 Ibid.
89 Singer and Friedman, 64.
90 Schmidle, "The Digital Vigilantes," The New Yorker.
91 "Computer hacking and the criminal law," In Brief, https://www.inbrief.co.uk/offences/hacking-of-computers/.
92 Josephine Wolff, "When Companies Get Hacked, Should They Be Allowed to Hack Back?When Companies Get Hacked, Should They Be Allowed to Hack Back?," The Atlantic, last modified July 14, 2017, https://www.theatlantic.com/business/archive/2017/07/hacking-back-active-defense/533679/.
93 "Discussion Draft of Active Cyber Defense Certainty Act," U.S. Congressman Tom Graves, https://tomgraves.house.gov/uploadedfiles/discussion_draft_active_cyber_defense_certainty_act_2.0_rep._tom_graves_ga-14.pdf.
94 Wolff, "When Companies Get Hacked," The Atlantic.
95 Schmidle, "The Digital Vigilantes," The New Yorker.
96 Wolff, "When Companies Get Hacked," The Atlantic.

exactly which customers' information had been stolen. This way, the company would not need to go through the costly effort of re-securing the information of all customers, they could just spend the time and effort re-securing the information that they knew had been stolen.

A successful hack back also might allow the attribution of the original attack to be determined. Figuring out a hack's attribution means figuring what actor was behind it. This can be done by figuring out the geographical location of the server the original hacker is using.

Interestingly, one tech writer noted that the advantages to legalizing hack backs resemble legalizing marijuana. Like marijuana, the "status quo (with hack backs) isn't working in society," the "issue is getting worse and costing more law enforcement dollars," and is legal in some countries around the globe.[97]

Updating hack back laws would allow for governments to express clearer expectations about online behavior, and allow for less ambiguity as to which cases can be prosecuted. After all, Carpenter isn't the only actor to have hacked back. At least two other instances where companies have hacked back have been documented. In 2010, Google launched a "secret counteroffensive" to gain access to a computer in Taiwan after discovering that Chinese hackers broke into users' Gmail accounts.[98] Some banks are thought to have hired hackers in 2014 to crash servers being used by Iran.[99] Surely, the number of organizations who hack back will only grow.

However, there are also downsides to legalizing hack backs. One cybersecurity writer believes so strongly that hack backs should not be legalized that she dubbed the idea of it "the worst idea in cybersecurity."[100]

The legalization of hack backs has been much-challenged because it's difficult to execute a successful hack back. It's difficult to determine the attribution of an attack, and as a result, an individual might inadvertently hack back at an innocent third party, or accidentally interfere with an ongoing government investigation that they're unaware of. It's difficult for those who hack back to determine in advance what they're going up against–they might mistakenly pick or escalate fights they can't actually win, and so get themselves into more trouble than it's worth.

97 Dan Lohrmann, "Hack Back Law: Why the Future May Be Like the Legalization of Marijuana," Government Technology, last modified September 22, 2017, http://www.govtech.com/blogs/lohrmann-on-cybersecurity/hack-back-law-why-the-future-may-be-like-the-legalization-of-marijuana.html.

98 David E. Sanger and John Markoff, "After Google's Stand on China, U.S. Treads Lightly," The New York Times, last modified January 15, 2010, https://www.nytimes.com/2010/01/15/world/asia/15diplo.html?ref=technology.

99 Wolff, "When Companies Get Hacked," The Atlantic.

100 Josephine Wolff, "Attack of the Hack Back," Slate, last modified October 17, 2017, http://www.slate.com/articles/technology/future_tense/2017/10/hacking_back_the_worst_idea_in_cybersecurity_rises_again.html.

There's also the problem of judging whether a hack back is justified or not, or whether those executing the hack back have gone too far with their hack back and been too aggressive and careless.

Those who are against legalizing hack backs think that at the end of the day, there are more effective ways of mitigating the effects of being hacked, such as the other solutions suggested earlier in this section. They believe we shouldn't worry about hack backs until we can ensure those methods are enacted. It can also be argued that hack backs do not get at the root of the problem; A successful hack back may ensure one hacker goes down, but as in whack-a-mole, another hacker will inevitably rise up.[101]

For these reasons, some actors in the cybersecurity community believe that hack backs should remain illegal, as legalizing them would cause more trouble than not.

Conclusion

These past actions and possible solutions are only a small sample of all that can be done to combat cybercrime. Some solutions will doubtless be more effective than others; These solutions will be the ones that fully consider the many factors that affect why cybercrimes are committed. There is no "silver bullet" for stopping cybercrimes altogether. Rather, the best solutions will consider the incentives and costs that drive cybercriminals to commit crimes, as well as what motivates governments, private firms, and individuals to defend against cyberattacks.

101 Singer and Friedman, 64.

A Bloc Positions

The debates over the Convention on Cybercrime and the International Telecommunications Union Treaty, both mentioned in the previous section, reflect countries' competing views of cybercrime fairly well. Certain countries, like the US, Australia, and Japan, resisted the passing of the ITU Treaty because they wanted to preserve the openness of the internet and not make it susceptible to being censored by more authoritarian states.[102] Meanwhile, more authoritarian states, like Russia, China, and Sudan, advocated for the passing of the ITU Treaty since it would allow for greater regulation of the internet and ultimately allow for greater sovereignty to be exercised over the internet as well.[103]

Thus, there are two main competing visions of the internet—one held by more authoritarian countries, and another held by more democratic countries. In addition, how advanced a country's cyber capabilities are, no matter whether that country is more authoritarian or democratic, affects its view on cybersecurity.

More authoritarian countries

In addition to a country wanting to create a political narrative by repressing what its citizens can share, a country may want to maintain sovereignty over its internet so that it can better promote the disinformation it may want to share, and increase its influence. For example, in 2014, Russia's spy agency, in an effort to win over public opinion to support its annexation of the Crimean peninsula, created fake social media profiles that supposedly were ordinary Ukrainian citizens, and commented messages of support for the pro-Russian Ukrainian president who had

102 Singer and Friedman, 184.
103 Singer and Friedman, 183.
104 Simon Denyer, "The Internet was supposed to foster democracy. China has different ideas.," The Washington Post, last modified July 10, 2016, https://www.washingtonpost.com/world/asia_pacific/the-internet-was-supposed-to-foster-democracy-china-has-different-ideas/2016/07/10/42954bbc-1dd9-11e6-b6e0-c53b7ef63b45_story.html?noredirect=on&utm_term=.7f96ea584663.

remarks are barred or censored," South China Morning Post, last modified April 21, 2016, https://www.scmp.com/news/

just been overthrown. In this way, Russia used social media to support its hopes of territorial expansion.[107]

Russia's disinformation campaign also underscores the fact that many non-Western countries are concerned about the internet's growing influence. Many non-Western countries view the internet as an inherently Western creation, and are worried that the West will try to proselytize through the internet.

More democratic countries

One key reason that democratic countries want to protect the openness of the internet is to preserve the free spread of information. Free speech is one of the pillars of a democracy, and the argument goes that if it is protected in print like it is with newspapers, it should also be protected online. The internet should be free not only so private citizens can express their own opinions truthfully, but also so dissidents and journalists can be protected.

In addition, many of these democratic countries are Western countries who believe that a more open internet can only assist in spreading culture or even Western influence. Also, a more open internet would give more opportunities to businesses like those in Silicon Valley to do business and profit.[108]

A note about countries with advanced cyber capabilities vs. countries with developing cyber capabilities

It is important to consider the fact that, on the whole, countries with more advanced cyber capabilities will be less likely to favor a cyber treaty that limits the use of cyber weapons, or a cyber treaty that criminalizes more acts.[109]

Once again, going back to the example of Stuxnet, this makes sense, because states that have more advanced cyber capabilities that they can utilize in state-sanctioned cyberattacks will be reluctant to handicap themselves. (This would be the cyber equivalent of willingly engaging in an arms control treaty when the other side hasn't shown you that they have any weapons.) For countries with advanced cyber capabilities, creating a cyber treaty that criminalizes certain cyberattacks will only give countries with developing cyber capabilities a chance to catch up.

Thus, it would be in the interest of states that are democratic powerhouses to encourage a safer, freer internet, and support a treaty that criminalizes certain actions, at least on paper. It is also

107 Ellen Nakashima, "Inside a Russian disinformation campaign in Ukraine in 2014," The Washington Post, last modified December 25, 2017, https://www.washingtonpost.com/world/national-security/inside-a-russian-disinformation-campaign-in-ukraine-in-2014/2017/12/25/f55b0408-e71d-11e7-ab50-621fe0588340_story.html?utm_term=.da3462afd931.

108 "There May Soon Be Three Internets. America's Won't Necessarily Be the Best.," The New York Times, last modified October 15, 2018, https://www.nytimes.com/2018/10/15/opinion/internet-google-china-balkanization.html.

109 Singer and Friedman, 186.

in the interest of more developed countries to push for stronger cybersecurity, especially since they tend to be more reliant on information systems for banking and governmental matters.

However, it is also in their interest to continue those possibly criminalizable actions, especially if they can't be caught. More authoritarian states may wish to question the more democratic states on their position on this particular topic.

Glossary

Cyber-dependent cybercrime: Crimes that can only be committed through the use of information and communications technologies such as telephone and computer networks.

Cyber-enabled cybercrime: Crimes that would be able to be committed without the use of information and communications technologies but whose scope and scale can be broadened with the use of ICT.

Information and communications technology: All modern technology that allows for interaction between people and organizations.

Phishing websites: Websites that attempt to fraudulently obtain people's sensitive information

Red teams: People, usually outside contractors, who are hired by a company to test how secure a company's defenses are.

Bibliography

Busvine, Douglas, and Stephen Nellis. "Security Flaws Put Virtually All Phones, Computers at Risk." Reuters. https://www.reuters.com/article/us-cyber-intel/security-flaws-put-virtually-all-phones-computers-at-risk-idUSKBN1ES1BO.

CDC. "Trends in the Prevalence of Behaviors That Contribute to Violence." Youth Risk Behavior Survey. https://www.cdc.gov/healthyyouth/data/yrbs/pdf/trends/2015_us_violence_trend_yrbs.pdf.

"Chart of signatures and ratifications of Treaty 185." Council of Europe. Last modified October 11, 2018. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures.

"Computer hacking and the criminal law." In Brief. https://www.inbrief.co.uk/offences/hacking-of-computers/.

"Convention on Cybercrime." Council of Europe. Last modified November 23, 2001. http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf.

Crown Prosecution Service. "Cybercrime - Prosecution Guidance." CPS Prosecution Guidance. Accessed July 9, 2018. https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance.

Denyer, Simon. "The Internet was supposed to foster democracy. China has different ideas." The Washington Post. Last modified July 10, 2016. https://www.washingtonpost.com/world/asia_pacific/the-internet-was-supposed-to-foster-democracy-china-has-different-ideas/2016/07/10/42954bbc-1dd9-11e6-b6e0-c53b7ef63b45_story.html?noredirect=on&utm_term=.7f96ea584663.

"Details of Treaty No.189." Council of Europe. Last modified January 28, 2003. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189.

"A digital cold war?" The Economist. Last modified December 14, 2012. https://www.economist.com/babbage/2012/12/14/a-digital-cold-war.

"Discussion Draft of Active Cyber Defense Certainty Act." U.S. Congressman Tom Graves. https://tomgraves.house.gov/uploadedfiles/discussion_draft_active_cyber_defense_certainty_act_2.0_rep._tom_graves_ga-14.pdf.

Drinkwater, Doug, and Kacy Zurkus. "Red team versus blue team: How to run an effective simulation." CSO. Last modified July 26, 2017. https://www.csoonline.com/article/2122440/disaster-recovery/emergency-preparedness-red-team-versus-blue-team-how-to-run-an-effective-simulation.html.

FBI. "Cyber Crime." What We Investigate. Accessed July 9, 2018. https://www.fbi.gov/investigate/cyber.

Gan, Nectar. "Xi Jinping calls for greater tolerance of criticism online about China's government ... and comments about his remarks are barred or censored." South China Morning Post. Last modified April 21, 2016. https://www.scmp.com/news/china/policies-politics/article/1937518/xi-jinping-calls-greater-tolerance-criticism-online.

Giles, Keir. "Russia's Public Stance on Cyberspace Issues." Last modified 2012. https://ccdcoe.org/publications/2012proceedings/2_1_Giles_RussiasPublicStanceOnCyberInformationWarfare.pdf.

Goldman, Zachary K. "Sanctioning Cyber Crime: The New Face of Deterrence." Council on Foreign Relations. Last modified May 19, 2015. https://www.cfr.org/blog/sanctioning-cyber-crime-new-face-deterrence.

Goodin, Dan. "At Facebook, zero-day exploits, backdoor code bring war games drill to life." Ars Technica. Last modified February 10, 2013. https://arstechnica.com/information-technology/2013/02/at-facebook-zero-day-exploits-backdoor-code-bring-war-games-drill-to-life/.

Jenkins, Nick. "The Hitchhiker's Guide to Bug Bounty Hunting Throughout the Galaxy." Medium. Last modified January 30, 2018. https://medium.com/@Nick_Jenkins/the-hitchhikers-guide-to-bug-bounty-hunting-throughout-the-galaxy-474ddb87ae15.

Lewis, James Andrew. "Economic Impact of Cybercrime." Center for Strategic & International Studies. Last modified February 21, 2018. Accessed July 9, 2018. https://www.csis.org/analysis/economic-impact-cybercrime.

Li, Johannes Xingan. "Cyber Crime and Legal Countermeasures: A Historical Analysis." *International Journal of Criminal Justice Sciences* 12, no. 2 (July-December 2017): 196-207. doi:10.5281/zenodo.1034658.

Lohrmann, Dan. "Hack Back Law: Why the Future May Be Like the Legalization of Marijuana." Government Technology. Last modified September 22, 2017. http://www.govtech.com/blogs/lohrmann-on-cybersecurity/hack-back-law-why-the-future-may-be-like-the-legalization-of-marijuana.html.

McGeehan, Ryan. "Red Teams." Medium. Last modified March 30, 2015. https://medium.com/starting-up-security/red-teams-6faa8d95f602.

Nakashima, Ellen. "Inside a Russian disinformation campaign in Ukraine in 2014." The Washington Post. Last modified December 25, 2017. https://www.washingtonpost.com/world/national-security/inside-a-russian-disinformation-campaign-in-ukraine-in-2014/2017/12/25/f55b0408-e71d-11e7-ab50-621fe0588340_story.html?utm_term=.da3462afd931.

Nakashima, Ellen, and Joby Warrick. "Stuxnet was work of U.S. and Israeli experts, officials say." *The Washington Post*, June 2, 2012. Accessed November 10, 2018. https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html?utm_term=.d72a98a491a4.

National Crime Agency. "Pathways into Cyber Crime." NCA Intelligence Assesment. Last modified January 13, 2017. Accessed July 9, 2018. http://www.nationalcrimeagency.gov.uk/publications/791-pathways-into-cyber-crime/file.

O'Brien, Dick. "A Short History of Law Enforcement and Cyber Crime." Medium. Last modified May 3, 2018. https://medium.com/threat-intel/cyber-crime-takedowns-66915be7307e.

Pappas, Stephanie. "Cyberbullying on Social Media Linked to Teen Depression." LiveScience. Last modified June 22, 2015. Accessed July 9, 2018. https://www.livescience.com/51294-cyberbullying-social-media-teen-depression.html.

Rouse, Margaret. "ICT (Information and Communications Technology, or Technologies)." TechTarget. Accessed July 9, 2018. https://searchcio.techtarget.com/definition/ICT-information-and-communications-technology-or-technologies.

Sanger, David E., and John Markoff. "After Google's Stand on China, U.S. Treads Lightly." The New York Times. Last modified January 15, 2010. https://www.nytimes.com/2010/01/15/world/asia/15diplo.html?ref=technology.

Schmidle, Nicholas. "The Digital Vigilantes Who Hack Back." The New Yorker. Last modified May 7, 2018. https://www.newyorker.com/magazine/2018/05/07/the-digital-vigilantes-who-hack-back.

Segal, Adam. *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age*. 2nd ed. New York, NY: Public Affairs, 2017.

Singer, P. W., and Allan Friedman. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. New York, NY: Oxford University Press, 2014.

Sterling, Bruce. *The Hacker Crackdown: Law and Disorder on the Electronic Frontier*. New York, NY: Bantam, 1992.

"STOP. THINK. CONNECT. ™." U.S. Department of Homeland Security. Last modified September 26, 2018. https://www.dhs.gov/stopthinkconnect.

"There May Soon Be Three Internets. America's Won't Necessarily Be the Best." The New York Times. Last modified October 15, 2018. https://www.nytimes.com/2018/10/15/opinion/internet-google-china-balkanization.html.

Tripathi, Rahul. "Home Ministry pitches for Budapest Convention on cyber security." The Indian Express. Last modified January 18, 2018. https://indianexpress.com/article/india/home-ministry-pitches-for-budapest-convention-on-cyber-security-rajnath-singh-5029314/.

United Nations. "Cybercrime Legislation Worldwide." United Nations Conference on Trade and Development. Accessed July 9, 2018. http://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Cybercrime-Laws.aspx.

"Global Programme on Cybercrime." United Nations Office on Drugs and Crime. Accessed July 9, 2018. https://www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html.

White, Rachael. "Cyber Security Breaches Cost British Businesses Almost £30 Billion in 2016." Beaming. Last modified March 1, 2017. Accessed July 9, 2018. https://www.beaming.co.uk/press-releases/cyber-security-breaches-cost-businesses-30-billion/.

Wolff, Josephine. "Attack of the Hack Back." Slate. Last modified October 17, 2017. http://www.slate.com/articles/technology/future_tense/2017/10/hacking_back_the_worst_idea_in_cybersecurity_rises_again.html.

"When Companies Get Hacked, Should They Be Allowed to Hack Back?When Companies Get Hacked, Should They Be Allowed to Hack Back?" The Atlantic. Last modified July 14, 2017. https://www.theatlantic.com/business/archive/2017/07/hacking-back-active-defense/533679/.

TOPIC B: THE ROLE OF SECRECY IN CRIME PREVENTION AND CRIMINAL JUSTICE

Statement of the Problem

Case Study 1: The Downfall of Silk Road

In 2013, the words **"Silk Road"** were buzzwords to any user of the dark web, a part of the web inaccessible by ordinary search engines like Google. The Silk Road in question was not a historical path but rather an online marketplace where over $1 billion of sales of illicit objects, mostly drugs, had taken place from 2011 to 2013. In that same time, nearly 1 million users had used the website.[110] The website's success was shocking, and so was the fact that its creator had evaded legal consequences thus far even though agents from the DEA, FBI, Homeland Security, IRS, Secret Service, and Postal Inspection Service had spent over a year trying to figure out and track down just who was behind it.[111]

The beginning of the end for Silk Road came when its creator, Ross Ulbricht, began interacting with a user whose username with Nob. Nob was not the aspiring drug seller he claimed to be, but rather a DEA agent named Mark Force posing as one.[112] Ulbricht's carelessness with Nob allowed law enforcement agencies to understand the seriousness of Ulbricht's offenses—at one point, Ulbricht had ordered Nob to kill a disloyal user of the site–and Force's scrutiny of his conversations with Ulbricht allowed him to track down and monitor Ulbricht's location.

However, law enforcement agents' reading of Ulbricht's messages also revealed that he had set up Silk Road's network so that he could destroy all evidence of his involvement with Silk Road with one keystroke. The agents pursuing Ulbricht knew that, as a result, acquiring Ulbricht's computer with all the evidence intact on it was crucial. So on October 1, 2013, when Ulbricht found himself in a California public library, a team of undercover FBI agents distracted him in order to seize his computer and arrested him afterwards. Ulbricht was caught in the act of sending a message on Silk Road to someone who was working for him. He was later sentenced to life in prison without the possibility of parole after a trial in which documents from his computer were used as evidence.[113][114]

110 "The Untold Story of Silk Road, Part 1 | WIRED," accessed November 12, 2018, https://www.wired.com/2015/04/silk-road-1/.
111 Ibid.
112 "The Untold Story of Silk Road, Part 2: The Fall | WIRED," accessed November 12, 2018, https://www.wired.com/2015/05/silk-road-2/.
113 Ibid.
114 "Recapping Week Two of the Silk Road Trial | TechCrunch," accessed November 12, 2018, https://techcrunch.com/2015/01/28/recapping-week-two-of-the-silk-road-trial/.

Case Study 2: Mass Surveillance and the NSA

Also in 2013, a security contractor for the National Security Agency (NSA) named Edward Snowden made headlines when he leaked classified information about mass surveillance programs that the NSA was running. Among the most heavily criticized programs were an initiative named XKeyscore, which allowed the NSA to search through vast online databases of users' personal emails, and an operation nicknamed Stellar Wind, where the NSA had access to users' phone data.[115] While the latter did not allow the NSA to access the content of users' phone calls, it allowed the NSA to collect data about everything else related to a call, known as metadata. Metadata includes details like the length of a call, the parties involved, and the locations of the parties involved.[116]

After Snowden leaked the extent of the NSA's surveillance programs, multiple review panels convened to review the efficacy of the programs in question. One of them reviewed whether the NSA's collection of bulk telephone records had stopped any terrorist attacks, and found that it had stopped exactly none.[117] While the metadata collection provided crime prevention agencies with some leads on terrorists' activities, it only made a significant difference in one case, where it revealed that a taxi driver had sent $8,500 to a Somalian terrorist group.[118] Furthermore, the collection was not only criticized by civil rights groups like the ACLU, but aspects of it were also found unconstitutional by a US District Judge in 2015.[119][120]

The NSA case raises the question of how a program that had so many resources at its disposal could be so ineffective. It raises the question of what is the point of gathering so much data that a single agency can't even sift through it all.

Introduction to the Problem: Secrecy and Crime Prevention

As the above examples demonstrate, secrecy can be a powerful tool for crime prevention agencies if used well. The use of secrecy in the first example allowed law enforcement agents to take down a criminal enterprise that was only growing larger by the day, and allowed the acquiring of evidence that was later used to prosecute someone. Meanwhile, the use of secrecy by the NSA in the second example has been criticized by many for abusing its power.

115 "XKeyscore: NSA Tool Collects 'Nearly Everything a User Does on the Internet' | US News | The Guardian," accessed November 13, 2018, https://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data.
116 "NSA Collected Americans' Email Records in Bulk for Two Years under Obama | US News | The Guardian," accessed November 13, 2018, https://www.theguardian.com/world/2013/jun/27/nsa-data-mining-authorised-obama.
117 "NSA Program Stopped No Terror Attacks, Says White House Panel Member," accessed November 13, 2018, https://www.nbcnews.com/news/world/nsa-program-stopped-no-terror-attacks-says-white-house-panel-flna2D11783588.
118 "Is This $8,500 Wire Transfer Really the NSA's Best Case for Tracking Americans' Phone Records? - The Washington Post," accessed November 13, 2018, https://www.washingtonpost.com/news/worldviews/wp/2013/08/09/is-this-8500-wire-transfer-really-the-nsas-best-case-for-tracking-americans-phone-records/?utm_term=.2ca599b7fe37.
119 "ACLU v. Clapper - Challenge to NSA Mass Call-Tracking Program," American Civil Liberties Union, accessed November 13, 2018, https://www.aclu.org/cases/aclu-v-clapper-challenge-nsa-mass-call-tracking-program.
120 "Judge Blocks NSA Spying and Sets an Important Precedent | WIRED," accessed November 13, 2018, https://www.wired.com/2015/11/judge-blocks-nsa-spying-and-sets-an-important-precedent/.

Conceptually, secrecy is a powerful tool. Most obviously, secrecy can be used as a means to conceal information. Or, in addition to using secrecy to deny the existence of something, it can also be used to mislead and deceive others. The use of secrecy at an organizational level is also important: the use of organizational security clearances, even when it doesn't actually allow those who have it to access sensitive information, gives those who possess them a sense of self-importance. An organization's use of secrecy can act as an initiation ritual for individuals; in organizations, secrecy can act as a badge of honor.[121]

In practice, secrecy is currently used by many agencies that are involved in crime prevention. Those agencies use secrecy in a variety of areas, including, but not limited to: secrecy in police fieldwork, espionage, the use of surveillance in crime prevention, and information sharing in crime prevention.

Secrecy and Police Work

Different levels of secrecy can be used in police work.

Secret police are established by national governments to maintain political and social control. They operate independently of the civil police, and because they have clearance from the government to perform extrajudicial actions like torture or deportation to suspected political enemies or opposition members, the use of secrecy is at its most extreme in these organizations. Some historical examples of secret police include the Russian KGB and the East German Stasi. Secret police tend to exist in less democratic nations, where it is possible for one political party can have total control over the government. [122]

Secrecy within police organizations exists in democratic nations as well, in a more moderate form. As the Silk Road case demonstrated, undercover police officers (who are permitted to lie about their status as a police officer if asked) can play a crucial role in foiling criminal plans.

However, there can be intangible gains to the police not using secrecy. In democratic nations, the use of secrecy in moderation by police can lead to police appearing more legitimate since they are respecting the rule of law. In this situation, people will be more likely to trust the police. This can make community members more willing to talk to police officers and share key pieces of evidence with them. Research has also shown that people are more likely to obey the law when they believe in the legitimacy and authority of police.[123]

121 Nuclear Rites, Hugh Gusterson
122 "Secret Police | Government Organization," Encyclopedia Britannica, accessed November 12, 2018, https://www.britannica.com/topic/secret-police.
123 "How to Build Trust in Policing," The Marshall Project, October 23, 2015, https://www.themarshallproject.org/2015/10/23/how-to-build-trust-in-policing.

Espionage

Certain activities are outlawed because their use of secrecy makes them dangerous and difficult to deal with. One example of this is **espionage**.

If you think about it, this example may be slightly puzzling: in the prior section, we established that it was possible, and perhaps even prudent, for law enforcement agents to sometimes shroud their identity in secrecy. However, when agents of one country cross the border into another country, the legal consequences they face, on the whole, are more severe.

The term espionage itself tends to be linked with illegality. One example of the definition of the word calls it the, "process of obtaining military, political, commercial, or other secret information by means of spies, secret agents, or illegal monitoring devices."[124] The main question and dilemma with espionage, then, is how a government can justify prosecuting individuals for using secrecy in acts like espionage, while that government itself uses secrecy in acts of surveillance.

Surveillance

Surveillance can happen overtly, like closed-circuit television systems (**CCTV**) in public places across a city, which provides video footage of those surveilled. CCTV cameras can serve as physical reminders to people that their actions are being monitored, which can help deter crime. In fact, a review of 41 research studies found that CCTV caused a drop in crime of about 16%.[125] In addition, CCTV can serve as a psychological reminder to residents that they are being watched, helping to shape their perceptions, attitudes, and behaviors.[126]

Surveillance can also happen more covertly as well. Examples of covert surveillance include wiretapping someone's phone without their knowledge or hacking into someone's webcam. The main question with surveillance, as with secrecy and police work, is where one draws the line between helpful surveillance and intrusive surveillance. What is to stop governments from

124 "Espionage | International Relations | Britannica.com," accessed November 12, 2018, https://www.britannica.com/topic/espionage.

125 "The Effect of CCTV on Public Safety: Research Roundup," *Journalist's Resource* (blog), February 11, 2014, https://journalistsresource.org/studies/government/criminal-justice/surveillance-cameras-and-crime.

126 Brandon C. Welsh and David P. Farrington, *How Might Surveillance Measures Reduce Crime?* (Oxford University Press, 2009), http://www.oxfordscholarship.com/view/10.1093/acprof:oso/9780195326215.001.0001/acprof-9780195326215-chapter-3.

abusing their powers like the way some argued the U.S. government did with the NSA a few years ago?

Conclusion

As shown above, secrecy is utilized in a multitude of ways within institutions whose mission is crime prevention; secrecy is also addressed in legislation having to do with such issues as espionage. If used to the correct degree, secrecy can be an efficient complement to other methods of crime prevention, as in the case of the undercover police agents taking down Silk Road. Meanwhile, the use of secrecy to an incorrect degree can not only be an inefficient crime prevention tool but also an exhibit as to how institutions may abuse their power when given too much of it, as in the case of the NSA's surveillance programs.

Should this topic be chosen, the major question that this committee will try to answer is how crime prevention and criminal justice agencies should balance the positives of secrecy with the negatives. Delegates are thus encouraged to write clauses that suggest guidelines for when agencies should stop using secrecy. Ultimately, it is important to consider that both granting institutions the ability to use too much secrecy and the ability to use too little secrecy is harmful.

A Note

It is important to note that while the content of this background guide mostly focuses on the use of secrecy as it pertains to police forces, legislation, and surveillance, these are only just a few of the uses of secrecy in crime prevention. Speeches and clauses about topics related to secrecy and crime prevention not mentioned here are very much welcome.

History of the Problem

Secrecy and police work

One of the most well-known historical examples of a secret police force is the Gestapo of Nazi Germany, an acronym for *Geheimstaatspolizei*, or "Secret State Police." It was formed after the Nazis rose to power in 1933. That year, all German police forces were combined, creating a national police organization for the first time (there had been Gestapo equivalents in individual German states in the past). The Gestapo's mission was, "to assure the effective battle against all endeavors directed at the existence and security of the state."[127] As the Nazis eliminated their political opponents and Adolf Hitler controlled the state through a dictatorship starting in 1934, the Gestapo were responsible for arresting anyone deemed to be an, "enemy of the state," including Jewish people, Roma, and homosexuals, and deporting them to extermination camps across German-occupied Europe.[128][129]

Though the Gestapo are one of the most well-known examples of a secret police, the number of people they actually employed was relatively low: only 32,000 people worked for them, and 18,500 were involved in policing.[130] Thus, most of their power came from informants and relying on denunciations from local populations that were inspired by propaganda the Nazi party pushed.[131]

Secret police still exist in some countries today. One example of a secret police is the 610 Office in China, named for the date it was founded: June 10, 1999.[132] The 610 Office's main duties involve monitoring the activities of and persecuting practitioners of Falun Gong, a Chinese spiritual practice drawn from Taoist principles, as the Chinese Communist party sees the independent teachings of Falun Gong as a threat to the state.[133] The 610 Office's power is so great that it has the ability to capture Falun Gong adherents and put them in "reeducation", or forced labor detention camps. While the 2001 Pulitzer Prize for International Reporting was awarded to a journalist who covered the 610's persecution of Falun Gong practitioners, little international attention has been paid to it since then. In March 2018, the 610 Office was moved to a different Ministry within the Chinese government, but it is unclear if this reduced its power.[134]

127 "Gestapo," accessed November 12, 2018, https://encyclopedia.ushmm.org/content/en/article/gestapo.
128 "The Nazi Rise to Power," accessed November 12, 2018, https://encyclopedia.ushmm.org/content/en/article/the-nazi-rise-to-power.
129 "Gestapo | Nazi Political Police," Encyclopedia Britannica, accessed November 12, 2018, https://www.britannica.com/topic/Gestapo.
130 Ibid.
131 "Foundations of the Nazi State," accessed November 12, 2018, https://encyclopedia.ushmm.org/content/en/article/foundations-of-the-nazi-state.
132 "The 610 Office: Policing the Chinese Spirit," Jamestown, accessed November 12, 2018, https://jamestown.org/program/the-610-office-policing-the-chinese-spirit/.
133 Ibid.
134 "Chinese Regime Breaks Up Gestapo-like Police," accessed November 12, 2018, https://www.theepochtimes.com/chinese-regime-breaks-up-gestapo-like-police_2476868.html.

Organized undercover police work has existed as early as the early 19th century, when Eugène François Vidocq set up the Security Brigade under the Paris Prefecture of Police. As a former criminal himself, Vidocq was an expert in knowing how to train his agents to lead undercover operations.[135] Meanwhile, England's first police force was founded in 1829 and used undercover officers since its founding. Because citizens worried about undercover officers having the power to politically repress people, an act passed in 1845 said that police superintendents had to personally approve all uses of undercover officers. However, officers frequently ignored these commands, leading the commissioner of the London Metropolitan Police to publicly rebuke his police in a trial.[136]

Secrecy and espionage

Espionage has existed in a variety of forms since ancient times. For example, the final chapter in Sun Tzu's *The Art of War,* written in the 5th century BC, is entitled "The Use of Spies."[137]

However, the concept of espionage really began to enter the international consciousness with the occurrence of the Dreyfus affair at the turn of the twentieth century. During this time, Alfred Dreyfus, a Jewish captain in the French army, was falsely convicted of handing the German government French military secrets. The Dreyfus affair was not only significant because it triggered a wave of anti-Semitism in France, but also because it highlighted the difficulty of restraining the state's power when it came to prosecuting spies: when the head of the army's intelligence unit uncovered evidence that showed Dreyfus was innocent and told his bosses this, he was transferred to North Africa and later imprisoned. It was not until 1906, twelve years after Dreyfus was convicted, that he was exonerated.[138]

As the importance of espionage was recognized, countries began to develop agencies that specialized in its use. In 1889, Field Marshal Helmuth von Moltke established a military intelligence unit to the German General Staff.[139] And in Britain, the Secret Service Bureau was established in 1909. It was made up of 19 military departments, from MI1 to MI19, and MI5 and MI6 from among them still remain active to this day.[140]

Many well-known cases of espionage occurred during the Cold War. One such case was that of Aldrich Hazen Ames. Ames was an underperforming CIA officer who became a KGB double

135 "François Vidocq | French Detective | Britannica.com," accessed November 12, 2018, https://www.britannica.com/biography/Francois-Eugene-Vidocq.
136 Rachael Griffin, *Detective Policing and the State in Nineteenth century England: The Detective Department of the London Metropolitan Police, 1842-1878*, PDF, p 230.
137 "The Art of War by Sun Tzu - Chapter 13: The Use of Spies," accessed November 12, 2018, https://suntzusaid.com/book/13.
138 Elizabeth Nix, "What Was the Dreyfus Affair?," HISTORY, accessed November 12, 2018, https://www.history.com/news/what-was-the-dreyfus-affair.
139 Walter T. Hitchcock, *The Intelligence Revolution*, PDF, United States Air Force Academy, p. 18.
140 "The Establishment Of The Secret Service Bureau | MI5 - The Security Service," accessed November 12, 2018, https://www.mi5.gov.uk/the-establishment-of-the-secret-service-bureau.

agent after a contact offered him money to reveal the names of CIA agents who were stationed in Moscow. Ames continued to give names to the KGB even after he found out he was causing the CIA agents he informed on to be arrested and executed.[141]

Ames was ultimately paid $4.6 million by the Soviets, making him the highest-paid spy in US history. When the CIA eventually became suspicious of how Ames could afford a luxury home worth half a million dollars and discovered what Ames had done, he was sentenced to life imprisonment without parole in federal prison. Meanwhile, the Russian intelligence agency station chief in Washington, who was also aware of and complicit in Ames's actions, was not prosecuted at all, since he possessed diplomatic immunity.[142] What is important to take away from Ames's story, then, is how diplomatic immunity can complicate the issue of espionage: it can protect those who flagrantly abuse it, unless the diplomat's immunity is revoked. This, however, is a complex process. Host states cannot take away the diplomat's immunity– the most that they nations can usually do is expel the diplomat, and arrest them if they ever return. Thus, it is usually up to the nation of the diplomat's origin to revoke immunity.[143]

Laws that have been passed to prosecute acts of espionage have also been used to prosecute non-spies. For example, the United States passed the Espionage Act of 1917 that criminalized any act that was the conveying of information with intent to interfere with the success of the country's armed forces.[144] The Espionage Act was passed with the intent of criminalizing the act of causing a threat to national security by passing information to someone not cleared to have it. However, Eugene Debs, the perennial Socialist Party presidential candidate, was convicted in 1921 under the Espionage Act for giving a speech that discouraged people from joining the Army.[145]

More recently, the Espionage Act has been used to convict whistleblowers like Daniel Ellsberg, who leaked the Pentagon Papers, Chelsea Manning, who leaked sensitive documents to Wikileaks, and Edward Snowden, who leaked classified information about the NSA.[146]

141 "An Assessment of the Aldrich H. Ames Espionage Case and Its Implications for U.S. Intelligence - Senate Select Committee on Intelligence - 01 November 1994 - Part One," accessed November 12, 2018, https://fas.org/irp/congress/1994_rpt/ssci_ames.htm.

142 James Risen, "Rules of Espionage: Got Caught? You Lose Players," *The New York Times*, March 23, 2001, sec. World, https://www.nytimes.com/2001/03/23/world/rules-of-espionage-got-caught-you-lose-players.html.

143 Christopher Beam, "How Far Does Diplomatic Immunity Go?," Slate Magazine, April 8, 2010, https://slate.com/news-and-politics/2010/04/how-far-does-diplomatic-immunity-go.html.

144 History com Editors, "U.S. Congress Passes Espionage Act," HISTORY, accessed November 12, 2018, https://www.history.com/this-day-in-history/u-s-congress-passes-espionage-act.

145 "HARDING FREES DEBS AND 23 OTHERS HELD FOR WAR VIOLATIONS; Socialist Leader's Sentence of Ten Years Is Commuted, Effective Christmas. NO RESTORATION OF RIGHTS None of 'Political' Prisoners Regains Citizenship--Some Are to Be Deported. FIVE EX-SOLDIERS PARDONED Men Serving Life Sentences for Murder of British Officer Released by President. - The New York Times," accessed November 12, 2018, https://www.nytimes.com/1921/12/24/archives/harding-frees-debs-and-23-others-held-for-war-violations-socialist.html?mtrref=en.wikipedia.org.

146 "Once Reserved For Spies, Espionage Act Now Used Against Suspected Leakers," NPR.org, accessed November 12, 2018, https://www.npr.org/sections/parallels/2017/06/28/534682231/once-reserved-for-spies-espionage-act-now-used-against-suspected-leakers.

The United States is not the only nation that has restricted the free speech of those who interfere with the government's use of secrecy in crime prevention and in other matters. Australia recently introduced and passed an espionage bill that gives it the power to punish would-be whistleblowing by criminalizing the act of printing, copying, or making notes from a sensitive document.[147]

Secrecy and surveillance

Perhaps the most obvious and recognized form of state surveillance is surveillance performed through a surveillance camera. Closed-circuit television systems (CCTV) were invented in 1942 by a German engineer who wanted to be able to monitor V2 rocket launches.[148] Since then, many cities have set up CCTV cameras to monitor activity in public places, with London being the most surveilled city in the world with 51,000 police cameras.[149] Today, the ratio of citizens to surveillance cameras in the United Kingdom overall is 11 to 1, raising questions about the cost efficiency of the practice.[150] Even small cities like Elk Grove in California have been spending hundreds of thousands of dollars to purchase systems that not only record footage but allow for detailed analysis of said footage. For example, a police officer in Elk Grove can do a facial search the footage recorded from all sources across the city if he wants to construct the previous path of an individual.[151]

In addition to video surveillance, governments can perform audio surveillance through wiretapping. In 1928, the Supreme Court established the constitutionality of wiretapping in Olmstead v. United States, but later overturned itself in 1967 in Katz v. United States, stating that a "reasonable" expectation of protection was afforded to people under the Fourth Amendment. [152][153] Notable examples of U.S. government wiretapping include the FBI's wiretapping of Dr. Martin Luther King, Jr.'s home from 1963 to 1966, as well as then-President Richard Nixon's authorization of the wiretapping of four reporters and 13 government officials in 1969.[154] Today, there are many differences of judicial opinion in the United States on the legality of exactly when wiretapping is allowed.[155]

147 "How Australia's Espionage Laws Could Silence Whistle-Blowers and Activists - The New York Times," accessed November 12, 2018, https://www.nytimes.com/2018/01/30/world/australia/australia-espionage-law.html.
148 "When Was CCTV Invented?," CCTV.co.uk, November 17, 2016, https://www.cctv.co.uk/when-was-cctv-invented/.
149 "The Most Spied Upon Cities in the World," WorldAtlas, accessed November 12, 2018, https://www.worldatlas.com/articles/most-spied-on-cities-in-the-world.html.
150 "One Surveillance Camera for Every 11 People in Britain, Says CCTV Survey - Telegraph," accessed November 12, 2018, https://www.telegraph.co.uk/technology/10172298/One-surveillance-camera-for-every-11-people-in-Britain-says-CCTV-survey.html.
151 "In More Cities, A Camera On Every Corner, Park And Sidewalk," NPR.org, accessed November 12, 2018, https://www.npr.org/sections/alltechconsidered/2013/06/20/191603369/The-Business-Of-Surveillance-Cameras.
152 "Olmstead v. United States," Oyez, accessed November 12, 2018, https://www.oyez.org/cases/1900-1940/277us438.
153 "Katz v. United States," Oyez, accessed November 12, 2018, https://www.oyez.org/cases/1967/35.
154 "Brief History: Wiretapping - TIME," accessed November 12, 2018, http://content.time.com/time/magazine/article/0,9171,2022653,00.html.
155 David H. Hines, *Fourth Amendment Limitations on Eavesdropping and Wire-Tapping*, PDF, Cleveland State University.

Past Actions and Possible Solutions

Some general guidelines on crime prevention

A compendium of standards and norms in crime prevention and criminal justice published by the United Nations Office on Drugs on Crime in 2006 provides some general guidelines on crime prevention.

The compendium outlines four broad methods. Firstly, there is *prevention through social development or social crime prevention*: the promoting of, "the well-being of people and [encouraging of] pro-social behaviour through social, economic, health and educational measures, with a particular emphasis on children and youth, and focus on the risk and protective factors associated with crime and victimization." Following this method with respect to the use of secrecy in crime prevention would involve paying attention to which groups of people are particularly in danger of suffering negative consequences from secrecy's use.[156]

The second method is *locally based crime prevention*. This asks someone to "change the conditions in neighbourhoods that influence offending, victimization and the insecurity that results from crime by building on the initiatives, expertise and commitment of community members." This method is more in conflict with the use of secrecy, since it involves fostering trust between law enforcement officers and community members.[157]

The third method is *situational crime prevention*, while involves, "reducing opportunities (for crime), increasing risks of being apprehended (for criminals), minimizing benefits, and offering assistance to victims." Secrecy can help to supplement this method, since if those being surveilled do not know when exactly they are being surveilled, they may be less likely to commit a crime since they are unsure of whether they can get away with reaping the benefits from it.[158]

Finally, the fourth method is *reintegration programs*—assisting in social awareness of offenders in order to prevent recidivism.[159]

Balancing secrecy and publicity

A comparison, written by Jeffrey Davis, between the existing legal guidelines of the United States and the United Kingdom, as well as European international law, demonstrates the different ways that states balance secrecy with publicity in courts.

156 *Compendium of United Nations Standards and Norms in Crime Prevention and Criminal Justice*, PDF, Vienna: UNITED NATIONS OFFICE ON DRUGS AND CRIME, p. 294-5.
157 Ibid, 295.
158 Ibid.
159 Ibid.

In the United States, state secrets privilege allows the Executive Branch to, "withhold evidence in civil cases or even demand dismissal of those cases based on the claim that disclosure would damage national security."[160] While this sounds reasonable in theory, in practice, the state secrets privilege has been applied very broadly. For example, in 2004, a German citizen named Khalid El-Masri claimed that he had been drugged by the CIA, flown to Kabul, Afghanistan, and tortured there. After he was released on an abandoned road, El-Masri filed a civil claim against the former Director of the CIA. However, government lawyers convinced the court to dismiss the case on the grounds of the state secrets privilege. Since the judge for the case reasoned, "the very subject of the litigation is itself a state secret," no steps could be taken to protect the secret material, and thus the case had to be dismissed.[161] El-Masri had no choice but to back down from legal action against the US.

More tellingly, the US Supreme Court ruled, in *Jeppesen v. US* in 1953, that courts do not need to require the government to produce evidence before a judge alone for the judge to determine if the privilege is warranted. While the dissenting judges in *Jeppesen* argued that the state secrets privilege can only be used to prohibit the introduction of specific evidence and not to dismiss entire cases before any evidence has been requested, the majority opinion of *Jeppesen* still stands true in the US today.[162]

Meanwhile, in the United Kingdom, the public interest immunity doctrine also allows for certain state secrets to be inadmissible as evidence to a trial. In contrast to the US's state secrets privilege, however, the standard interpretation of the public interest immunity doctrine only allows for any secret evidence in question to be excluded from a trial after extensive review by a trial judge, rather than for the entire dismissal of a case to happen. Thus, the application of the public interest immunity doctrine is less broadly applied than the state secrets privilege.[163]

Secrecy and information sharing

How private or public crime prevention and law enforcement agencies choose to go about their ongoing projects and investigations can affect the efficacy of those investigations.

A crime prevention agency's decision to share information with the public may lead to the public being alert and able to help "crowdsource" the investigation and share tips with the investigative agency. For example, although they have often been criticized for not being effective enough, AMBER alerts, the emergency response system that shares information through phone notifications and electronic roadway signs, have helped save over 500 missing or abducted

160 Davis, p 60
161 Davis, p 68-69
162 Davis, p. 66-67
163 Davis, p. 65

children since they were introduced in 1996.[164] Crime prevention agencies sharing information with the public may also help strengthen trust between the two, making it more likely that non-agency members will be willing to help a crime prevention agency in the future.[165]

Other times, an agency sharing information with the public may only generate noise and distraction. For example, in the aftermath of the Boston Marathon bombing in the United States, internet users took to Reddit and tried to figure out the identity of the Boston Marathon bomber from photos that were released. In the ensuing discussion, two innocent people were illogically accused by Redditors of being the Boston Marathon bomber. One of the accused was so terrified of the scrutiny that he refused to leave his home.[166]

Another thing to consider is that when an agency chooses to keep the details of an investigation secret, it often makes it harder for journalists to hold agencies accountable to both their citizens and the international community at large. However, agencies choosing to keep the details of an investigation secret often intentionally do this having kept that in mind--they often want to keep the inner workings of their agencies an enigma to the international community.[167]

Another scenario where the sharing of information by a crime prevention agency may be crucial is when it is in their interest to do so with another agency. Though the initiation of information sharing by an agency may make it seem weak, increases in efficiency gained from the action can be huge. For example, currently within in the United States, the Department of Homeland Security's Law Enforcement Information Sharing Service provides its federal, state, local, tribal, and international partners with access to more than 2.6 million subject records.[168] Nearly 500 institutions participate in the program, and it has contributed to a change in law enforcement culture and willingness to share information.[169]

164 "15 Years Later, Critics Debate Effectiveness of Amber Alert," Washington Post, accessed November 12, 2018, https://www.washingtonpost.com/national/15-years-later-critics-debate-effectiveness-of-amber-alert/2011/01/21/ABDZX0G_story.html.

165 Richard V. Ericson, "Patrolling the Facts: Secrecy and Publicity in Police Work," *The British Journal of Sociology* 40, no. 2 (1989): 205–26, https://doi.org/10.2307/590269.

166 "Should Criminal Investigations Be Crowdsourced? - CNN," accessed November 12, 2018, https://www.cnn.com/2013/04/22/tech/web/boston-suspects-reddit-sleuthing/index.html.

167 "Project MUSE - Uncloaking Secrecy: International Human Rights Law in Terrorism Cases," accessed November 12, 2018, https://muse.jhu.edu/article/609302/pdf.

168 "Law Enforcement Information Sharing Initiative | ICE," accessed November 12, 2018, https://www.ice.gov/le-information-sharing.

169 "Law Enforcement Information Sharing," accessed November 12, 2018, https://www.dni.gov/index.php/who-we-are/organizations/ise/ise-archive/ise-additional-resources/2142-law-enforcement-information-sharing.

Bloc Positions

Americas

Secrecy has played a role in the governmental fabric of the United States of America since pre-revolutionary times; Espionage, counterintelligence, and covert actions played massively into revolutionary tactics, and these strategies continued to evolve throughout the following decades.[170] Today, espionage and covert operations continue to play a massive role in the criminal systems of North and South American countries, both within national borders and across them. In particular, the United States has sent several spies into Latin-American nations, and vice-versa. One example of this was the arrest and incarceration of Ana Montez, a former American senior analyst at the Defense Intelligence Agency of the United States. In 2001, Montez was arrested and charged with conspiracy to commit espionage after it had been discovered that she had been sending and receiving encrypted transmissions to and from the Cuban government. Montez was accused of passing a considerable amount of classified information along to the Cuban intelligence Directorate, information that included the identities of four US spies undercover in Cuba at the time. As of 2018, Montez remains incarcerated, to be released in 2023.[171]

One of the largest fields in which covert operations have been employed in in recent years in North America is in the so-called "War on Drugs," an ongoing and contentious campaign led by the United States aimed at reducing illegal drug trading within the US. The United States has worked in conjunction with several other countries in the Americas, including Mexico, Honduras, and Guatemala, in attempts to mitigate the production, distribution, and consumption of illegal drugs across borders. There have been several covert measures taken throughout the span of the campaign, including information-sharing between nations, undercover operations, and several raids on traffickers' sites of operation.[172] As these examples show, espionage and secrecy are deeply rooted in the criminal systems of countries in the Americas. With this in mind, delegates in this bloc will need to assess the extent to which secrecy will continue to play into their foreign and domestic affairs.

Africa

As resource extraction in Africa by the west has increased in the 21st century, so has its role as a hub for international espionage. Though African states do not conduct much intelligence gathering of their own, many African nations serve as hot-spots for other countries to come

170 "History of American Intelligence — Central Intelligence Agency," accessed November 10, 2018, https://www.cia.gov/kids-page/6-12th-grade/operation-history/history-of-american-intelligence.html.
171 Jim Popkin (2013-04-18), "Ana Montes did much harm spying for Cuba. Chances are, you haven't heard of her," *Washington Post Magazine*, The Washington Post.
172 "A New Front Line in the U.S. Drug War," *New York Times*, May 31, 2012.

in and set up shop to conduct spy activities. The US and other western states have expanded their presence on the continent in recent years, capitalizing in particular on the increasing communicative powers of South Africa. This can be seen, for instance, in the fact that South African intelligence agencies spend a large amount of time and resources digging into Iran and jihadist groups, although the South African government does not consider either a major threat to South Africa itself. The National Intelligence Agency of South Africa has also reported on the activity of countries in other African nations.[173]

Delegates representing African nations must consider what they feel their role in international and domestic espionage should be: Should focus remain on serving as a hub for other nations to conduct their spying through, or should African nations view this involvement as an underminement to their national sovereignty and strive to become more involved in decisions regarding secrecy on the global stage?

Asia

The use of espionage is deeply rooted in the histories of several Asian countries, and it continues to be a widely-used tool for Asian nations today. China's government is thought to be highly engaged in espionage directed through the Ministry of State Security, mostly with the goal of gaining commercial, technological, and military secrets.[174] China's spying programs are rather unique in that they often utilize academics or students rather than long-term, cultivated double agents. Another key tactic employed in Chinese espionage is cyber-spying, which allows remote access to sensitive information, though the use of physical agents is common as well.[175] China has operations on almost every continent, with notable influence in the rest of Asia. India's intelligence service, the Research and Analysis Wing, has informed companies to stop using Chinese-made telecommunication equipment for fear of it having spy capabilities embedded within it.[176] Japan's Public Security Intelligence Agency, established in 1952, focuses on conducting surveillance and collecting information regarding potential threats from terrorist groups and other potential spy agencies. This agency has several cooperative foreign ties as well — including to the American Central Intelligence Agency and the Research and Analysis Wing of India — which allow operatives to train together and share analysis techniques.[177] Since secrecy and espionage are so prevalent within the region, delegates in this bloc will need to consider how their nation feels the role of espionage should evolve on the global stage when

173 Seumas Milne and Ewen MacAskill, "Africa Is New 'El Dorado of Espionage', Leaked Intelligence Files Reveal," *The Guardian*, February 24, 2015, sec. World news, https://www.theguardian.com/world/2015/feb/24/africa-el-dorado-espionage-leaked-intelligence-files.
174 Olivia Ward (6 June 2007). "Ex-envoy warns of Chinese spies," *Toronto Star*, Retrieved 2008-04-08.
175 David Johnston (23 May 1999), "The Nation; Finding Spies Is the Easy Part," *The New York Times*.
176 "UPI Asia, India's telecom agency raises china spy scare, 8 October 2009," Upiasia.com, 2012-07-22.
177 "Public Security Investigation Agency [Koancho]," accessed November 10, 2018, https://www.globalsecurity.org/intell/world/japan/koancho.htm.

it comes to crime prevention and criminal justice, and how exactly they can contribute to this growth and development.

Europe

Historically, European nations have produced some of the most infamous secret police teams in the world, like the KGB in Russia and the Gestapo in Germany. European nations have come a long way from organizations like these, but the role of secrecy in European governments remains prominent overall today. Intelligence agencies are all over Europe, and many European nations have several different branches or divisions of intelligence agencies. The European Union even formed the European Union Intelligence and Situation Centre in 2012 as a way to provide information and ensure situational awareness to participating EU member states.[178] In addition to contributing to the realm of secrecy and espionage, many European nations are also the prime targets for subterfuge. The United Kingdom in particular has been labelled as one of the prime targets for intelligence gathering, with foreign governments seeking military, industrial, and political secrets that could potentially be used to their advantage.[179] Since delegates in this bloc represent nations that both heavily engage in and are frequently targeted by covert operations, they must consider what stances and measures they are willing to take in order to both ensure their own interests and protect their governments against the interests of others.

Middle East

Historically, covert operations have played an important role in many Middle Eastern nations. The use of intelligence gathering was integral to the unification of Saudi Arabia in the early 1900s.[180] Currently, Saudi Arabia's primary intelligence agency is the General Intelligence Directorate. This agency has remained prominent throughout the 21st century as an organization deeply involved in regional espionage; The agency's involvement as of late has centered around the civil war in Syria, and even more recently, the death of journalist Jamal Khashoggi has brought international attention to the intelligence agency.[181] [182] Some intelligence agencies within the region, such as Iran's Ministry of Intelligence, have unclear functions and goals.[183] This governmental agency sprung from the more infamous former Iranian intelligence agency SAVAK, which was established in the 1950s after the installation of Mohammad Reza Shah as leader of the country. SAVAK had essentially unlimited power within the country, and was heavily involved in collecting information on political opponents and repressing dissident movements. Upon the fall of the

178 "Select Committee on European Union Seventh Report. Appendix 5. Joint Situation Centre (JSC)".
179 "The UK Is a High Priority Espionage Target. | Public Website," accessed November 11, 2018, https://www.cpni.gov.uk/espionage.
180 Max Fisher (November 2010), "What We Can Learn From Saudi Intelligence," *The Atlantic*.
181 Anthony Cordesman (2006), Saudi Arabia: National Security in a Troubled Region, Center for Strategic and International Studies, p. 234.
182 Saphora Smith (25 October 2018), "Saudis change Khashoggi story again, admit killing was 'premeditated,'" NBC News.
183 "Iran - SAVAMA," accessed November 11, 2018, http://www.country-data.com/cgi-bin/query/r-6549.html.

Shah, the Iranian government ushered in the Ministry of Intelligence as a replacement for SAVAK, and although the new regime aimed to move away from the deeply covert nature of SAVAK, the new agency remained highly secretive.[184] In addition to operations within countries in this bloc, several other nations (the US in particular) have led covert operations and intelligence-gathering measures within the region. One of the more notable of such instances was the 1953 coup in Iran staged by the American CIA and United Kingdom.[185] Based on the historical and current attitudes concerning secrecy and espionage within this region, delegates representing countries within this bloc will need to consider the extent of their roles within and outside the region when it comes to issues of secrecy.

184 Nikki R. Keddie and Yann Richard, *Modern Iran: Roots and Results of Revolution* (Yale University Press, 2006), p. 134.
185 "Special Report: Secret History of the CIA in Iran," *New York Times*, 2000.

Glossary

Espionage: The practice of spying or of using spies, typically by governments to obtain political and military information.

CCTV systems: Closed-circuit television systems that can serve as a means of surveillance by collecting public spaces on video.

The Silk Road: The first modern online black market, best known as a platform for selling illegal drugs.

Bibliography

"15 Years Later, Critics Debate Effectiveness of Amber Alert." Washington Post. Accessed November 12, 2018. https://www.washingtonpost.com/national/15-years-later-critics-debate-effectiveness-of-amber-alert/2011/01/21/ABDZX0G_story.html.

"A New Front Line in the U.S. Drug War." *New York Times*. May 31, 2012.

"ACLU v. Clapper - Challenge to NSA Mass Call-Tracking Program." American Civil Liberties Union. Accessed November 13, 2018. https://www.aclu.org/cases/aclu-v-clapper-challenge-nsa-mass-call-tracking-program.

"An Assessment of the Aldrich H. Ames Espionage Case and Its Implications for U.S. Intelligence - Senate Select Committee on Intelligence - 01 November 1994 - Part One." Accessed November 12, 2018. https://fas.org/irp/congress/1994_rpt/ssci_ames.htm.

Beam, Christopher. "How Far Does Diplomatic Immunity Go?" Slate Magazine, April 8, 2010. https://slate.com/news-and-politics/2010/04/how-far-does-diplomatic-immunity-go.html.

"Brief History: Wiretapping - TIME." Accessed November 12, 2018. http://content.time.com/time/magazine/article/0,9171,2022653,00.html.

"Chinese Regime Breaks Up Gestapo-like Police." Accessed November 12, 2018. https://www.theepochtimes.com/chinese-regime-breaks-up-gestapo-like-police_2476868.html.

Cordesman, Anthony (2006). Saudi Arabia: National Security in a Troubled Region. Center for Strategic and International Studies. p. 234.

Editors, History com. "U.S. Congress Passes Espionage Act." HISTORY. Accessed November 12, 2018. https://www.history.com/this-day-in-history/u-s-congress-passes-espionage-act.

Ericson, Richard V. "Patrolling the Facts: Secrecy and Publicity in Police Work." *The British Journal of Sociology* 40, no. 2 (1989): 205–26. https://doi.org/10.2307/590269.

"Espionage | International Relations | Britannica.com." Accessed November 12, 2018. https://www.britannica.com/topic/espionage.

"Foundations of the Nazi State." Accessed November 12, 2018. https://encyclopedia.ushmm.org/content/en/article/foundations-of-the-nazi-state.

"François Vidocq | French Detective | Britannica.com." Accessed November 12, 2018. https://www.britannica.com/biography/Francois-Eugene-Vidocq.

Fisher, Max (November 2010). "What We Can Learn From Saudi Intelligence". *The Atlantic*.

"Gestapo." Accessed November 12, 2018. https://encyclopedia.ushmm.org/content/en/article/gestapo.

"Gestapo | Nazi Political Police." Encyclopedia Britannica. Accessed November 12, 2018. https://www.britannica.com/topic/Gestapo.

"HARDING FREES DEBS AND 23 OTHERS HELD FOR WAR VIOLATIONS; Socialist Leader's Sentence of Ten Years Is Commuted, Effective Christmas. NO RESTORATION OF RIGHTS None of 'Political' Prisoners Regains Citizenship--Some Are to Be Deported. FIVE EX-SOLDIERS PARDONED Men Serving Life Sentences for Murder of British Officer Released by President. - The New York Times." Accessed November 12, 2018. https://www.nytimes.com/1921/12/24/archives/harding-frees-debs-and-23-others-held-for-war-violations-socialist.html?mtrref=en.wikipedia.org.

"History of American Intelligence — Central Intelligence Agency." accessed November 10, 2018. https://www.cia.gov/kids-page/6-12th-grade/operation-history/history-of-american-intelligence.html.

"How Australia's Espionage Laws Could Silence Whistle-Blowers and Activists - The New York Times." Accessed November 12, 2018. https://www.nytimes.com/2018/01/30/world/australia/australia-espionage-law.html.

"How to Build Trust in Policing." The Marshall Project, October 23, 2015. https://www.themarshallproject.org/2015/10/23/how-to-build-trust-in-policing.

"In More Cities, A Camera On Every Corner, Park And Sidewalk." NPR.org. Accessed November 12, 2018. https://www.npr.org/sections/alltechconsidered/2013/06/20/191603369/The-Business-Of-Surveillance-Cameras.

"Is This $8,500 Wire Transfer Really the NSA's Best Case for Tracking Americans' Phone Records? - The Washington Post." Accessed November 13, 2018. https://www.washingtonpost.com/news/worldviews/wp/2013/08/09/is-this-8500-wire-transfer-really-the-nsas-best-case-for-tracking-americans-phone-records/?utm_term=.2ca599b7fe37.

"Iran - SAVAMA." Accessed November 11, 2018. http://www.country-data.com/cgi-bin/query/r-6549.html.

Johnston, David (23 May 1999). "The Nation; Finding Spies Is the Easy Part". *The New York Times*.

"Judge Blocks NSA Spying and Sets an Important Precedent | WIRED." Accessed November 13, 2018. https://www.wired.com/2015/11/judge-blocks-nsa-spying-and-sets-an-important-precedent/.

"Katz v. United States." Oyez. Accessed November 12, 2018. https://www.oyez.org/cases/1967/35.

Keddie, Nikki R. and Yann Richard. *Modern Iran: Roots and Results of Revolution* (Yale University Press, 2006). p. 134.

"Law Enforcement Information Sharing." Accessed November 12, 2018. https://www.dni.gov/index.php/who-we-are/organizations/ise/ise-archive/ise-additional-resources/2142-law-enforcement-information-sharing.

"Law Enforcement Information Sharing Initiative | ICE." Accessed November 12, 2018. https://www.ice.gov/le-information-sharing.

Milne, Seumas, and Ewen MacAskill. "Africa Is New 'El Dorado of Espionage', Leaked Intelligence Files Reveal." *The Guardian*, February 24, 2015, sec. World news. https://www.theguardian.com/world/2015/feb/24/africa-el-dorado-espionage-leaked-intelligence-files.

Nix, Elizabeth. "What Was the Dreyfus Affair?" HISTORY. Accessed November 12, 2018. https://www.history.com/news/what-was-the-dreyfus-affair.

"NSA Collected Americans' Email Records in Bulk for Two Years under Obama | US News | The Guardian." Accessed November 13, 2018. https://www.theguardian.com/world/2013/jun/27/nsa-data-mining-authorised-obama.

"NSA Program Stopped No Terror Attacks, Says White House Panel Member." Accessed November 13, 2018. https://www.nbcnews.com/news/world/nsa-program-stopped-no-terror-attacks-says-white-house-panel-flna2D11783588.

"Olmstead v. United States." Oyez. Accessed November 12, 2018. https://www.oyez.org/cases/1900-1940/277us438.

"Once Reserved For Spies, Espionage Act Now Used Against Suspected Leakers." NPR.org. Accessed November 12, 2018. https://www.npr.org/sections/parallels/2017/06/28/534682231/once-reserved-for-spies-espionage-act-now-used-against-suspected-leakers.

"One Surveillance Camera for Every 11 People in Britain, Says CCTV Survey - Telegraph." Accessed November 12, 2018. https://www.telegraph.co.uk/technology/10172298/One-surveillance-camera-for-every-11-people-in-Britain-says-CCTV-survey.html.

Popkin, Jim (2013-04-18), "Ana Montes did much harm spying for Cuba. Chances are, you haven't heard of her." *Washington Post Magazine*. The Washington Post.

"Project MUSE - Uncloaking Secrecy: International Human Rights Law in Terrorism Cases." Accessed November 12, 2018. https://muse.jhu.edu/article/609302/pdf.

"Public Security Investigation Agency [Koancho]." accessed November 10, 2018. https://www.globalsecurity.org/intell/world/japan/koancho.htm.

"Recapping Week Two of the Silk Road Trial | TechCrunch." Accessed November 12, 2018. https://techcrunch.com/2015/01/28/recapping-week-two-of-the-silk-road-trial/.

Risen, James. "Rules of Espionage: Got Caught? You Lose Players." *The New York Times*, March 23, 2001, sec. World. https://www.nytimes.com/2001/03/23/world/rules-of-espionage-got-caught-you-lose-players.html.

"Secret Police | Government Organization." Encyclopedia Britannica. Accessed November 12, 2018. https://www.britannica.com/topic/secret-police.

"Select Committee on European Union Seventh Report. Appendix 5. Joint Situation Centre (JSC)".

"Should Criminal Investigations Be Crowdsourced? - CNN." Accessed November 12, 2018. https://www.cnn.com/2013/04/22/tech/web/boston-suspects-reddit-sleuthing/index.html.

Smith, Saphora (25 October 2018). "Saudis change Khashoggi story again, admit killing was 'premeditated'". NBC News.

"Special Report: Secret History of the CIA in Iran". *New York Times*. 2000.

"The 610 Office: Policing the Chinese Spirit." Jamestown. Accessed November 12, 2018. https://jamestown.org/program/the-610-office-policing-the-chinese-spirit/.

"The Art of War by Sun Tzu - Chapter 13: The Use of Spies." Accessed November 12, 2018. https://suntzusaid.com/book/13.

"The Commission on Crime Prevention and Criminal Justice." Accessed November 13, 2018. http://www.unodc.org/unodc/en/commissions/CCPCJ/index.html.

"The Effect of CCTV on Public Safety: Research Roundup." *Journalist's Resource* (blog), February 11, 2014. https://journalistsresource.org/studies/government/criminal-justice/surveillance-cameras-and-crime.

"The Establishment Of The Secret Service Bureau | MI5 - The Security Service." Accessed November 12, 2018. https://www.mi5.gov.uk/the-establishment-of-the-secret-service-bureau.

"The Most Spied Upon Cities in the World." WorldAtlas. Accessed November 12, 2018. https://www.worldatlas.com/articles/most-spied-on-cities-in-the-world.html.

"The Nazi Rise to Power." Accessed November 12, 2018. https://encyclopedia.ushmm.org/content/en/article/the-nazi-rise-to-power.

"The UK Is a High Priority Espionage Target. | Public Website." Accessed November 11, 2018. https://www.cpni.gov.uk/espionage.

"The Untold Story of Silk Road, Part 1 | WIRED." Accessed November 12, 2018. https://www.wired.com/2015/04/silk-road-1/.

"The Untold Story of Silk Road, Part 2: The Fall | WIRED." Accessed November 12, 2018. https://www.wired.com/2015/05/silk-road-2/.

"UN Commission on Crime Prevention and Criminal Justice | GIP Digital Watch." Accessed November 13, 2018. https://dig.watch/actors/un-commission-crime-prevention-and-criminal-justice.

"UPI Asia, India's telecom agency raises china spy scare, 8 October 2009". Upiasia.com. 2012-07-22.

Ward, Olivia (6 June 2007). "Ex-envoy warns of Chinese spies". *Toronto Star*. Retrieved 2008-04-08.

Welsh, Brandon C., and David P. Farrington. *How Might Surveillance Measures Reduce Crime?* Oxford University Press, 2009. http://www.oxfordscholarship.com/view/10.1093/acprof:oso/9780195326215.001.0001/acprof-9780195326215-chapter-3.

"When Was CCTV Invented?" CCTV.co.uk, November 17, 2016. https://www.cctv.co.uk/when-was-cctv-invented/.

"XKeyscore: NSA Tool Collects 'Nearly Everything a User Does on the Internet' | US News | The Guardian." Accessed November 13, 2018. https://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data.