

## Committee Overview

Since 1948, the United Nations Legal Committee, otherwise known as the Sixth Committee, has met to make decisions regarding international law. This committee was created to address Chapter IV, Article 13 of the UN Charter, specifically it seeks to “encourage the progressive development of International Law and its codification.”<sup>1</sup> The UN Charter is the founding document of the United Nations, and it is this document that committees and the United Nations itself largely derive their authority from. It is a committee in the UN General Assembly, and as such all UN member states may participate in it.<sup>2</sup>

The Legal Committee has previously addressed issues that affect the entire world, including maritime law, laws regarding diplomats, and laws regarding terrorism. However, decisions made by this committee are non-binding, as they are simply recommendations.<sup>3</sup> This means that countries are not required to follow the recommendations of the Legal Committee, so countries that engage in activities that the committee sees as violations of international law are unlikely to cease these activities. However, the committee’s decision is still quite powerful, as it helps to establish a precedent for seeing certain actions or activities as illegal, and in addition countries that do not engage in potentially illegal activities are somewhat likely to follow recommendations or at least take them into account. In other words, while the Legal Committee cannot unilaterally stop violations of international law, it can certainly help to sway opinions and get some countries to follow the law.

## Drone Warfare

### The History of Drone Warfare

The first true drone to be used in combat was a relatively simple aircraft designed by the Germans during World War II to be used against British cities. It was a vengeance weapon, one designed to destroy British infrastructure, lives, and morale, within the constraints Germany was facing during 1944 and 1945, although its construction had begun earlier. Although this drone, the

V-1 flying bomb, shares little in common with the drones of today, its use could be seen as the grandfather of modern day drone warfare.<sup>4</sup> After the V-1, drones were largely relegated to reconnaissance roles, although drone technology was used to convert old planes into targets for experimental weapons. The only combat roles drones occupied were similar to those the V-1 was used for, one way missions designed to deliver a warhead carried inside of the drone. However, since the War on Terror started after the September 11<sup>th</sup> attacks on the World Trade Centers, drones have increasingly been used in combat roles, usually as tools to assassinate suspected terrorists and terrorist leaders.

In the War on Terror, drones originally served in relatively limited roles. They surveyed the battlefield, and occasionally participated in strikes to support ground forces. In Afghanistan, the CIA is said to have been flying unarmed drones since 2000. However it was not until 2002 when the CIA first used an unmanned Predator drone in a targeted killing. The strike occurred in Afghanistan's Paktika province and was supposed to kill Osama Bin Laden. Despite the fact that the U.S had used drones long before that attack, and even during the air war against the Taliban in 2001, the CIA had not yet used a drone for a strike outside military support. The 2002 attack was the first pure CIA kill operation, undertaken separately from any military operations that were ongoing at that time.<sup>5</sup> Since then, the CIA has used drones in order to assassinate suspected terrorists. Under the Obama administration, the number of strikes has not only been increased, the strikes have also become more public. Many people, including Americans, question the morality and legality of using drones to kill suspected terrorists abroad.<sup>6</sup> In a report written by Christof Heyns, the UN Special Rapporteur on extrajudicial, summary or arbitrary executions, he stated that "only a State's highest authority can give permission to another State to use force on its territory and if that permission is withdrawn, such force must cease."<sup>7</sup> This statement is particularly relevant to the War on Terror, as drone strikes are regularly conducted in Pakistan, while Pakistani courts have found that these strikes

are technically illegal. On the other hand, others point out the fact that drones offer the military an excellent platform for counterterrorism, that is, they are great tools for fighting terrorism especially in foreign countries. Drones can loiter longer than many other options, and are generally fairly precise. However, the biggest advantage for many is the fact that the use of drones keeps American troops safe by eliminating the need to send them on possibly dangerous assassination missions. They are arguably even benefits for the countries that drones are used in, as drones could be considered less invasive than the invasions and occupations they help to replace.

Drones have also begun to proliferate in other ways as their ability to replace humans in roles besides reconnaissance has increased. Many nations still operate drones for reconnaissance purposes, with others, such as the US and UK, using drones for strike purposes. But drones have also begun to branch out more. The US Navy is already considering adopting an autonomous fighter jet, although this would not occur for at least 20 years. Drones have also been considered for use in ground combat, instead of the aerial role they have generally been used in.

However, despite many countries desires to expand drone operations, other countries have instead moved to prevent the use of drones, with armed drones generally drawing the most ire. This ire is often tied into the debate over counterterrorism, with activists opposing the use of drones because of their use in targeted killings. However, there is a fair bit of disagreement on how much should be banned, with some groups wanting to ban all armed drones, while others only want to ban armed drones that are fully autonomous. These groups see the immediate future as the best time to advocate for bans on armed drones, as drones may proliferate greatly when other countries begin to develop indigenous drone designs, and in order to stop autonomous drones from being armed to begin with, as it may be more difficult to prevent that after they begin to be deployed.<sup>8</sup> But while these groups oppose the use of armed drones, most do not oppose the use of military drones in

general. It appears that at least for reconnaissance purposes, the world has accepted that drones are a better alternative than manned planes.

For most of the time that they have been used, drones have had a human controlling the aircraft. Even now, drones are flown by pilots, although this is usually only for the critical parts of a mission, and the pilot is generally based in the United States. But recently efforts have been made to develop completely autonomous drones, with one successfully demonstrating the ability of a completely autonomous aircraft to land on an aircraft carrier.<sup>9</sup> The US military wishes to develop autonomous drones as they would reduce personnel costs, and might be better than humans at certain tasks. For example, drones are much better at resisting g-forces than humans, which increases the aircraft and gives it an edge in close range combat. Drones in general are cheaper to buy than piloted aircraft, although future air superiority drones may end up being just as expensive as a piloted version of the same craft. The savings on personnel might make it worth it though, as drones would not need to be paid wages, or have medical conditions treated, or perhaps most importantly, would not need to be trained. The US military is strongly considering the benefits offered by drones, and it is actually possible that the US Navy's next fighter aircraft will at least have an unmanned option, as the program to acquire such aircraft accepts unmanned entries. However, even if the decision is made to use unmanned aircraft, the earliest this would occur would be around 2025.<sup>10</sup>

### The Current Status of Drone Warfare

Addressing the legality of drones is very important. Right now drones operate in a sort of legal gray area, they are legal, but they are often used to break or bend international law. The UN has acknowledged this, and encouraged countries to use them within the bounds of the law.<sup>10</sup> By crafting resolutions to address the issues involved in drone warfare, countries can expand their drone fleets without having to worry about the lack of laws regarding these tools, and their use in battle can be

specifically proscribed, which may help to prevent the sorts of deaths that have led drones to be reviled by some groups. Of course, these resolutions would have far ranging effects, particularly on the US and its allies, as the War on Terror has been fought in large parts by these drones and their operators. Of course, while it is smart to look at previous uses of drones, such as their use in the War on Terror, do not forget that the War on Terror may not accurately represent the future of armed drones. Resolutions will almost certainly also affect major defense companies, as they hope to sell large amounts of drones to countries that desire the benefits drones offer. These economic effects would be widespread as well, with American companies such as Northrop Grumman, French companies such as Dassault Aviation, Israeli companies such as Israel Aerospace Industries, and Russian companies such as Mikoyan all producing drones for military use. However, these companies are all major aerospace firms, so it is unlikely that drone legislation or Legal Committee recommendations would cause their bankruptcy. Resolutions could still affect small companies though, as restrictions on combat drones may also dampen enthusiasm for civilian drone use.

#### Current Analysis of Drone Warfare

Drones currently occupy an interesting legal space right now, as mentioned before, they are currently legal, but some countries use them to flout international law. A full ban on armed drones would be appealing to some, but some of the biggest countries that already use armed drones may be unwilling to give them up so easily. Autonomous drones specifically could be banned, or their use limited, but this may affect the development of technology in this area due to a lack of military incentive to develop it further. The military provides significant funding for developing technologies like drones, so forbidding militaries from acquiring autonomous drones could prevent their development by cutting off the main source of funding of their development programs. Alternatively, the Committee could require greater oversight of drones, instead of banning anything

specifically, however enforcement may be an issue if this route is taken. These potential solutions and others should be considered to address the issues brought up by drones during our committee.

### Questions to Consider

Is the use of drones in combat, whether autonomous or simply unmanned, ethical?

Is it acceptable to use drones for some purposes, and to ban them from serving other purposes?

Should drone strikes have the oversight that a Special Forces operation would have over it?

How much should a country be required to inform other countries of its drone operations?

Should the development of autonomous combat drones be allowed to continue?

Is it feasible to enforce greater oversight of combat drones?

Do drones represent a dangerous technology that must be addressed, or is it simply their use that is problematic?

Is the potential of drones to save lives worth the legal and ethical issues their use brings up?

### Further Reading

These sources should not form the entirety of your research, but they do provide a starting point that should show you a variety of viewpoints on the topic.

1. <http://www.e-ir.info/2013/07/18/just-war-theory-and-the-ethics-of-drone-warfare/>, This piece by Erich Freiberger looks at whether drone warfare is ethical.

2. <http://peacepolicy.nd.edu/2013/03/28/moral-legal-challenges-of-drone-warfare/>, This piece by David Cortright shows opinions of some others on drones, specifically drone strikes, and whether they are ethical or legal.

3. <http://www.economist.com/node/21524876>, This article by the Economist argues that the use of drones does not violate the rules of war.

4. [http://www.nytimes.com/2012/07/15/sunday-review/the-moral-case-for-drones.html?\\_r=0](http://www.nytimes.com/2012/07/15/sunday-review/the-moral-case-for-drones.html?_r=0), This article by Scott Shane argues that using drones is actually the moral thing to do.

5. <http://www.pbs.org/wnet/religionandethics/2012/03/02/august-26-2011-the-ethics-of-drones/9350/>, This PBS report by Kim Lawton also looks at the ethics of the sort of drone warfare conducted by the United States.

### End Notes

1. "Charter of the United Nations," Last modified June 26, 1945, Digital file.
2. United Nations, "UN General Assembly - Legal Committee," UN General Assembly, Accessed August 22, 2014, <http://www.un.org/en/ga/sixth/index.shtml>.
3. "History of the Sixth Committee," Saint Peter's University, accessed August 22, 2014, [http://archive.saintpeters.edu/PDFfiles/Guarini\\_Center/legal.pdf](http://archive.saintpeters.edu/PDFfiles/Guarini_Center/legal.pdf).
4. John Sifton, "A Brief History of Drones," *The Nation*, February 27, 2012, [Page #].
5. "Fi-103/V-1 'Buzz Bomb,'" Warbirds Resource Group, last modified 2013, accessed July 16, 2014, <http://www.warbirdsresourcegroup.org/LRG/v1.html>.
6. Jack Serle, "More than 2,400 Dead as Obama's Drone Campaign Marks Five Years," The Bureau Investigates, last modified January 23, 2014, accessed July 16, 2014, <http://www.thebureauinvestigates.com/2014/01/23/more-than-2400-dead-as-obamas-drone-campaign-marks-five-years/>.
7. Chris Cole, "Drone Warfare and International Law: Findings of U.N. Reports on Extrajudicial and Arbitrary Executions," Global Research, last modified October 26, 2013, accessed July 16, 2014, <http://www.globalresearch.ca/drone-warfare-findings-of-u-n-reports-on-extrajudicial-and-arbitrary-executions/5355601>.
8. Elsa Rossbach, "How Europeans Are Opposing Drone and Robot Warfare: An Overview of the Anti-Drone Movement in Europe," Truth-out, last modified November 8, 2013, accessed August

22, 2014, <http://truth-out.org/news/item/19904-how-europeans-are-opposing-drone-and-robot-warfare-an-overview-of-the-anti-drone-movement-in-europe>.

9. "X-47B UCAS," Northrop Grumman, accessed July 16, 2014,

<http://www.northropgrumman.com/Capabilities/X47BUCAS/Pages/default.aspx>.

10. Christopher Cavas, "USN, Industry Seek New Concepts For 6th-generation Fighter," Defense News, <http://www.defensenews.com/apps/pbcs.dll/article?AID=2013307100015> (accessed September 27, 2014).

11. "UN Rights Experts Call for Transparency in the Use of Armed Drones, Citing Risks of Illegal Use," UN News Centre, last modified October 25, 2013, accessed August 22, 2014,

[http://www.un.org/apps/news/story.asp?NewsID=46338#.U\\_fy7PIdU1J](http://www.un.org/apps/news/story.asp?NewsID=46338#.U_fy7PIdU1J).

### Bibliography

Cavas, Christopher. "USN, Industry Seek New Concepts For 6th-generation Fighter." Defense News. <http://www.defensenews.com/apps/pbcs.dll/article?AID=2013307100015> (accessed September 27, 2014).

"Charter of the United Nations." Last modified June 26, 1945. Digital file.

Cole, Chris. "Drone Warfare and International Law: Findings of U.N. Reports on Extrajudicial and Arbitrary Executions." Global Research. Last modified October 26, 2013. Accessed July 16, 2014. <http://www.globalresearch.ca/drone-warfare-findings-of-u-n-reports-on-extrajudicial-and-arbitrary-executions/5355601>.

McManus, Doyle. "The Drone Warfare Drawbacks." Los Angeles Times. Last modified July 5, 2014. Accessed July 16, 2014. <http://www.latimes.com/opinion/op-ed/la-oe-mcmanus-column-drones-20140706-column.html>.

Northrop Grumman. "X-47B UCAS." Northrop Grumman. Accessed July 16, 2014. <http://www.northropgrumman.com/Capabilities/X47BUCAS/Pages/default.aspx>.

Rossbach, Elsa. "How Europeans Are Opposing Drone and Robot Warfare: An Overview of the Anti-Drone Movement in Europe." Truth-out. Last modified November 8, 2013. Accessed August 22, 2014. <http://truth-out.org/news/item/19904-how-europeans-are-opposing-drone-and-robot-warfare-an-overview-of-the-anti-drone-movement-in-europe>.

Saint Peter's University. "History of the Sixth Committee." Saint Peter's University. Accessed August 22, 2014. [http://archive.saintpeters.edu/PDFfiles/Guarini\\_Center/legal.pdf](http://archive.saintpeters.edu/PDFfiles/Guarini_Center/legal.pdf).

Serle, Jack. "More than 2,400 Dead as Obama's Drone Campaign Marks Five Years." The Bureau Investigates. Last modified January 23, 2014. Accessed July 16, 2014. <http://www.thebureauinvestigates.com/2014/01/23/more-than-2400-dead-as-obamas-drone-campaign-marks-five-years/>.

Sifton, John. "A Brief History of Drones." *The Nation*, February 27, 2012.

United Nations. "UN General Assembly - Legal Committee." UN General Assembly. Accessed August 22, 2014. <http://www.un.org/en/ga/sixth/index.shtml>.

———. "UN Rights Experts Call for Transparency in the Use of Armed Drones, Citing Risks of Illegal Use." UN News Centre. Last modified October 25, 2013. Accessed August 22, 2014. [http://www.un.org/apps/news/story.asp?NewsID=46338#.U\\_fy7PIdU1J](http://www.un.org/apps/news/story.asp?NewsID=46338#.U_fy7PIdU1J).

Warbirds Resource Group. "Fi-103/V-1 'Buzz Bomb.'" Warbirds Resource Group. Last modified 2013. Accessed July 16, 2014. <http://www.warbirdsresourcegroup.org/LRG/v1.html>.

## Cyber Espionage

### The History of Cyber-Espionage

For the majority of history, espionage has been a purely physical affair, with agents conducting groundwork inside a country. However, as the use of technology has spread, physical espionage has been replaced by technological espionage. Arguably, the first major example of this was during WWII, when British experts cracked the German enigma code, allowing the Allies to listen in on German radio communications. Since those times, the internet has largely replaced radio, and as such has begun to play a role in global espionage.

The potential for the computer's role in cyber espionage was demonstrated as early as the 1980's. During this time, the first PC virus, "Brain", was written by two brothers, Basit Farooq and Amjad Farooq, in Punjab, Pakistan. This virus, which, according to the brothers, had been written to protect their medical software from piracy and was only intended to target copyright infringers, would bury itself in the part of the disk that was needed for running programs and would infect any computer into which it was inserted. After that, the virus would remain in the computer's memory and infect any new disks that were inserted into that machine. In its code, however, it had the names, phone numbers and address of the brothers' shop. According to Amjad, "The idea was that

only if the program was illegally copied would the virus load", calling the bug a "friendly virus" and "not made to destroy data", much unlike those today. Around the same time, it was discovered that someone had released a malevolent computer program into the computer network. By the morning of November 3, 1988, thousands of computers were clogged with many copies of what would become known as a computer "worm", a program which would spread from computer to computer like a biological infection. The innovator behind this first worm was a graduate student at M.I.T named Robert Morris, who became one of the first people to be prosecuted and convicted under an anti-hacking statute that the U.S Congress had passed a couple of years earlier. The most significant effect that the worm had on the Internet, however, was that it forced software vendors to take security flaws in their products more seriously.

Since then, cyber espionage and cyber attacks have become more complex and more frequent. One example of this is the 1998 cyber-attack "Moonlight Maze", which was used to steal sensitive but unclassified information from the United States government. In this incident, which is thought to have come from Russia, United States officials found a pattern of probing of computer systems in agencies such as the Pentagon, NASA, and private universities and research labs. In response to these attacks, the United States Department of Defense was forced to implement stronger security procedures. Another example is Operation Aurora. This operation, first seen most by government entities and now by the private sector, has been designed to infect, conceal access, siphon data, and even modify data without detection. The "Moonlight Maze" and Operation Aurora attacks have reached a new level of sophistication by combining encryption, stealth programming and a hole that was unknown in Internet Explorer. "Moonlight Maze" and Operation Aurora were used to gain access to computer systems and then install and activate malware on those systems. The systems were then connected to a remote server in order to steal intellectual property from companies. In 2010, Google announced that it had been the target of sophisticated and coordinated

attacks such as these. Not long after, Adobe also released a statement saying that it too had been a victim of such attacks. Operation Aurora has demonstrated that all companies, both private and public, as well as governments, are vulnerable to attacks.

One of the most recent and threatening examples of the internet's new role in espionage is the case of the Chinese hackers' attacks on European and U.S businesses and government agencies, with a focus on the satellite, aerospace, and communications sectors. In a speech at the Chinese Academy of Sciences and Chinese Academy of Engineering, President Xi Jinping encouraged "indigenous innovation" and the end of Chinese dependence on Western technology. He described how China is pursuing their goal through great investments in science, technology, and education, and how in 2011, China surpassed Japan as the world's second largest spender on research and development. However, it has been said that the illicit transfer of intellectual property due to a lack of protection, industrial espionage, or cyber theft, additionally plays a role in Chinese efforts to strengthen the economy. These hackers are possibly employed by the Chinese military, and one of their main goals could be to steal information such as trade secrets from American companies, in order to strengthen the competitiveness of Chinese companies. However, the fact that these hackers are based in China, and employed by the Chinese military, makes countering them much harder. It is therefore incredibly difficult to persecute these hackers, as the Chinese government insists that they are not hacking anything, and that in fact it is America that is the hacker. In a speech, Vice Foreign Minister Li Baodong rejected U.S efforts to draw a line between political or military cyber espionage and cyber theft designed to steal intellectual property. "An individual country," stated Li, "has exercised double standards on the cyber issue, drawn lines out of its selfish interests and concocted 'regulations' only applicable to other countries." This sort of attitude prevents the US from extraditing the guilty parties and forcing them to stand trial.

The Chinese claims about American espionage activities are not entirely wrong. Since 2013, the US has found itself defending the NSA from attack after the whistleblower, Edward Snowden, released information on the agency's programs. This information revealed the extent to which the NSA went to gather information, which included spying on both US citizens and foreigners. Even close US allies, such as Germany and Brazil, were targeted, complicating diplomatic relationships as a result of this seeming betrayal. In a speech at United Nations headquarters in New York, Brazilian President Dilma Rousseff said on the topic of cyber espionage "What we have in front of us is a serious case of the violation of human rights and a lack of respect for the sovereignty of my country... Information and telecommunication technologies cannot be the new battlefield between states. Time is ripe to create the conditions to prevent cyberspace from being used as a weapon of war, through espionage, sabotage, and attacks against systems and infrastructure of other countries." Meanwhile, in the US itself, citizens felt betrayed that the government was able to observe their cyber activities without needing a warrant.

### The Current Status of Cyber Espionage

Due to its rapid growth in numbers and sophistication, the United Nations has recently begun to put more focus on the issue of cyber espionage. In 2011, the United Nations Economic and Social Council (ECOSOC) held a special event in New York focused on "Cybersecurity and Development". The discussion's goal was to build awareness by providing a picture of the current situation and challenges concerning cybersecurity, identifying a range of effective practice policies to build a culture of cybersecurity, and exploring possible options for a global response to cybercrimes. The role of economic disparities between nations was brought up, as well as the fact that developing countries do not have enough capacity to combat cybercrimes and cyber attacks. This lack of capacity could create "safe havens" where cyber criminals could take advantage of the lack of strong security measures. Additionally, there was talk of building upon the Budapest Convention, an

international treaty that seeks to harmonize national criminal laws of computer crimes such as fraud, child pornography, copyright infringement, and breaches of network security. Representatives at the 12th UN Congress on Crime Prevention discussed the possibility of the creation of a new international cooperation system to address the increasing dilemmas caused by cyber crimes. .

### Current Analysis of Cyber Espionage

Cyber crimes and cyber espionage have caused widespread debate. Some believe that it should be absolutely illegal, while others say it may be useful at times. Despite this, the increasing number and sophistication of bad-intended cyber espionage and crimes demands that actions be taken against it as soon as possible. Because technology is constantly changing, global legislation will not only have to catch up but also keep pace with criminal misuses. There is a great risk that countries with lower level of cybersecurity will be taken advantage of by cyber criminals for years to come. Therefore, international cooperation is essential in order to successfully prosecute and investigate cybercrimes. The fight against cyber crimes could also be fought using specialists information hubs and intelligence coordination. This could include analyzing the extent and harm of a cyber criminal groups' activities or protecting citizens against attacks. However, Brandon Valeriano of the University of Glasgow and Ryan Maness of the University of Illinois at Chicago, warn against over protection against cyber espionage threats. They state that "occasionally, when seeking secure forms of protection against cyber espionage, one may overreact and overprotect, cutting itself off from the systems and opportunities the global information age has done so well to create. Just as business has been harmed by terrorism, business itself has been just as hardened by cyber operations".

### Questions to Consider

1. Can parts of the internet be thought of as belonging to a country or a person?
2. Does a person's right to privacy extend to the internet?

3. How far can a country go to punish hackers and spies, even if they are based in another country?
4. What is the true scope of cyber espionage occurring today? Should countries be allowed to use their espionage technology on each other?
5. Where is the line between the "different" types of cyber espionage?
6. Is all cyber espionage the same?
7. Should all cyber espionage be treated with the same severity?
8. Can cyber espionage be morally justified in response to an attack from an enemy?
9. Can cyber espionage be justified during war?
10. Is cyber espionage a crime?

#### Endnotes

Baines, Victoria. "Fighting the Industrialization of Cyber Crime." *UN Chronicle*, August 2013.

Accessed August 22, 2014.

<http://unchronicle.un.org/article/fighting-industrialization-cyber-crime/>.

Bennett, Tess. "Brazil: President Rousseff Condemns Cyber Espionage at UN." *The Argentina*

*Independent*, September 24, 2013. Accessed August 22, 2014.

[http:// www.argentinaindependent.com/currentaffairs/brazil-president-rousseff-condemns](http://www.argentinaindependent.com/currentaffairs/brazil-president-rousseff-condemns)

-cyber-espionage-at-un/.

"The birth of the first personal computer virus, Brain." news.com.au. Last modified January 19, 2011. Accessed August 22, 2014.

<http://www.news.com.au/technology/the-birth-of-the-first-personal-computer-virus-brain/story-e6frfro0-1225990906387>.

"CASE STUDY: OPERATION AURORA." Triumfant Incorporated. Last modified 2010. Accessed August 22, 2014.

[http://www.triumfant.com/pdfs/Case\\_Study\\_Operation\\_Aurora\\_V11.pdf](http://www.triumfant.com/pdfs/Case_Study_Operation_Aurora_V11.pdf).

Lee, Timothy B. "How a grad student trying to build the first botnet brought the Internet to its knees." *Washington Post*, November 1, 2013. Accessed August 22, 2014.

<http://www.washingtonpost.com/blogs/the-switch/wp/2013/11/01/how-a-grad-student-trying-to-build-the-first-botnet-brought-the-internet-to-its-knees/>.

"NSA Spying on Americans." Electronic Frontier Foundation. Accessed August 22, 2014.

<https://www.eff.org/nsa-spying>.

Oltermann, Philip, and Spencer Ackerman. "Germany asks top US intelligence official to leave country over spy row." *The Guardian*, July 10, 2014. Accessed August 22, 2014.

<http://www.theguardian.com/world/2014/jul/10/germany-asks-top-us-intelligence-official-spy-row>.

PBS. "Cyber Wars." Frontline. Last modified April 24, 2003. Accessed August 22, 2014.

<http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/warnings/>.

Segal, Adam. "Chinese Cyber Espionage: We Still Don't Know What To Do About It." *Forbes*, June 11, 2014. Accessed August 22, 2014.

<http://www.forbes.com/sites/adamsegal/2014/06/11/weve-got-the-who-how-why-and-why-it-matters-of-chinese-cyber-espionage-still-missing-the-what-to-do/>.

Tiezzi, Shannon. "China's Response to the US Cyber Espionage Charges." *The Diplomat*, May 21, 2014. Accessed August 22, 2014.

<http://thediplomat.com/2014/05/chinas-response-to-the-us-cyber-espionage-charges/>.

Valeriano, Brandon, and Ryan Maness. "A Theory of Cyber Espionage for the Intelligence Community". PDF File. Accessed August 22, 2014.

[https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CB4QFjAA&url=https%3A%2F%2Fwww.usnwc.edu%2FAcademics%2FFaculty%2FDerek-Reveron%2FWorkshops%2FIntelligence%2C-National-Security-and-War%2FDocuments%2FManess.aspx&ei=z\\_f3U4jXKdf-yQSMoIGQDg&usg=AFQjCNEQcpYJLhBQI6sejk7qPmjvRXB1w&sig2=Hi1fREJbvXcYuw\\_T79CIYw&bvm=bv.73612305,d.aWw](https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CB4QFjAA&url=https%3A%2F%2Fwww.usnwc.edu%2FAcademics%2FFaculty%2FDerek-Reveron%2FWorkshops%2FIntelligence%2C-National-Security-and-War%2FDocuments%2FManess.aspx&ei=z_f3U4jXKdf-yQSMoIGQDg&usg=AFQjCNEQcpYJLhBQI6sejk7qPmjvRXB1w&sig2=Hi1fREJbvXcYuw_T79CIYw&bvm=bv.73612305,d.aWw)