PacificMUN 2017

Disarmament and International Security Committee (DISEC)

Backgrounder Guide

Topic A: Cyberwarfare

PacificMUN 2017

Dare to Speak | February 24–26 2017

Bryan Buraga
Secretary-General

Christopher Yuen
Deputy Secretary-General External

Timothy Ro
Deputy Secretary-General Internal

Alice Li
Chief of Staff

Elizabeth Vaz
Under Secretary-General of Delegate Affairs

Charles Balcita
Under Secretary-General of Committees 1

Alan Milligan
Under Secretary-General of Committees 2

Saad Yasin
Under Secretary-General of Conference

Jonathan Kim
Under Secretary-General of Finance

Shakil Jessa
Under Secretary-General of Sponsorship

Andy Wang
Under Secretary-General of Information Technology

Mingxin Gong
Under Secretary-General of Design and Media

Dear Delegates,

It is my honor and pleasure to invite you to the third session of Pacific Model United Nations and to serve as your Director for the First Committee of the United Nations General Assembly; the Disarmament and International Security Committee (DISEC).

Always being a avid MUNner myself, the idea of directing my own committee excites me beyond ever before. Personally, returning to General Assembly committees is very nostalgic for me, as I distinctly remember my first conference. It was a General Assembly and I was nervous beyond belief, afraid to talk in front of so many people for the first time ever. I remember being intimidated by the staff and admiring their prowess in being able to sit up there and direct a committee. Seeing now as I return to a General Assembly this time as a director myself I can recall my entire journey to be able to mold myself through all the MUN conferences I have been to. On day one of the conference when I am sitting in the dais chair and seeing all the nervous faces of first time delegates in the room, I will only be reminded of my first experience. Except this time, it will be different. It will be different because I do not want you to be intimidated or afraid of me and my fellow staff.

Instead, I encourage any delegate to think of me and my fellow staff as friends, people you can talk to about MUN and people who are happy to guide you through any question you have. When it comes down to it, everyone in MUN has had that first delegate experience, and I truly intend on making that experience an outstanding one for all first time delegates in my committee.

First time delegate or not, I encourage you to strive for your very best this conference. I know that I will and your fellow staff will as well. I entrust that you will all be well researched and eager to speak and participate in the committee. When February comes, I look forward to what each of you will discuss and talk about regarding Cyberwarfare and Drones.

I hope that all delegates will be able to take something away from the DISEC delegate experience this year at PacificMUN 2017. I am extremely excited to meet all of you then! Feel free to contact me with any comments or questions or even just to say hello.

All the best,
Dunstan Wang
Director, Disarmament and International Security Committee

DISEC was created to deal with disarmament, global challenges and threats to peace. It is meant to keep the international community safe and peaceful by using solutions in the international security regime[1].

The General Assembly was formed in 1945 when the United Nation (UN) Charter was first ratified. The General Assembly is one the main 6 organs of the UN and is the main deliberative, policymaking, and representative organ of the UN[2]. Each country has one vote in any General Assembly, and will consist of every member of the UN[3]. Important matters such as those on peace and security, admission of new members, or budgetary matters, require two thirds majority.[4] Other simpler matters only require simple majority.

DISEC is considered to play a major role in the General Assembly. The phrase "international peace and security" is mentioned six times in Chapter IV of the UN Charter. DISEC however does not hold the power to impose sanctions or allow for armed intervention[5]. It does however, hold the authority to initiate studies and pass resolutions for the purpose of international political cooperation as well as "the development and codification of international law.[6]" In a quick synopsis, DISEC cannot require countries to take a specific action. It can however make recommendations to the Security Council.

[1] http://www.un.org/en/ga/first/
[2] http://www.un.org/en/ga/about/
[3] http://www.un.org/en/sections/un-charter/chapter-iv/index.html
[4] Ibid
[5] http://www.unaslovenia.org/en/un/assembly2011
[6] Ibid

With the ever-growing expanse of technology and information this world is becoming more reliant by the second on the useful tool of the World Wide Web. The internet's usefulness is beyond compare, and the service it provides is outstanding. The powerful search engine Google processes an average of 40,000 searches per second. That translates to 1.2 trillion Google searches in a year[7].

But alas, like every good thing, the internet also has high potential for criminal activity and evil-doers. Vint Cerf, recognized as one of the fathers of the internet, once said, "The Internet is brittle and fragile and too easy to take down. It's a conduit for criminal activity. We need international treaties to prosecute the bad guys, but we don't have them.[8]" Cerf is exactly right. Terrorists, criminal organizations, and other countries are using the internet to wreak havoc across the planet.

Indonesia once mentioned that information and communication technology could be used for purposes that were inconsistent with maintaining international stability and security. Pakistan also stated that technological innovations had been used in recent years for indiscriminate surveillance and as a means of waging cyber-attacks. The Russian Federation said the prevention of political and military confrontation in terms of cyberwarfare was particularly urgent. No country can deny that cyberwarfare is a pressing threat to our society nowadays and all seem to agree that if unchecked, cyber warfare could topple the entire entity of International Security[9].

[7] http://www.internetlivestats.com/
[8] http://www.forbes.com/forbes/2011/0606/opinions-rich-karlgaard-innovation-rules-internet-guru.html
[9] http://www.un.org/press/en/2014/gadis3512.doc.htm

June 1982	The CIA obtained information about the Soviet Union plans to steal software from a Canadian company in order to control its Trans-Siberian Pipeline. They then altered the software to cause the pipeline to explode. This is considered to be the first cyberattack.
August 1986	Clifford Stoll, a physics researcher at the University of California at Berkeley, tracked down a hacker who had broke into computers at the Lawrence Berkeley National Laboratory, a U.S. Department of Energy facility, and other military computers in the U.S over the course of 10 months. Clifford traced the hacker to Germany. This is the first successful investigation of its kind.
November 1988	10% of the world's Internet servers are temporarily shut down by a worm. Robert Tappan Morris (Cornell student) released the worm and was the first person tried and convicted under the computer fraud and abuse act. It is the first occurrence of an Internet worm.
June 1997	A test known as the Eligible Receiver is conducted by the NSA to assess the vulnerability of government and military computers to a cyberattack. It revealed that systems throughout the country can be very easily hacked and disrupted.
April - May 2007	Estonia's government websites are compromised for 22 days due to distributed-denial-of-service (DDoS) attacks. Hackers are believed to be backed by the Russian government. Major targets are the president's office, Parliament, law enforcement officials, and two of the biggest banks in Estonia.
September 2007	Hackers breached the computers of the Foreign Office and other government agencies. China's People's Liberation Army are the believed perpetrators.
January 2009	During the conflict with Hamas in the Gaza Strip Israel's government Internet sites are attacked. As many as 15 million junk emails per second were sent to government computers and the computers were temporarily paralyzed. Israel suspects Hamas.
June 2010	Stuxnet is discovered. It is the world's first military-grade cyber weapon. It has the potential to destroy pipelines and cause explosions at power plants and factories and manipulate machinery. Stuxnet is the first worm that is able to corrupt industrial equipment. It is also the first worm to incorporate a programmable logic controller (PCL) which is software that is designed to hide the existence and progress of Stuxnet. In August 2010 the company Symantec states that 60% of all computers infected with Stuxnet are in Iran.[10]
February 2013	The United Nations released a comprehensive cybercrime study report for the purpose of identifying international standards of cybercrime and persecution of such crime[11].
June 2013	A panel discussion is held on cyber security in Germany[12].

[10] http://www.infoplease.com/world/events/cyberwar-timeline.html
[11] https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf
[12] https://www.eastwest.ngo/events/cybersecurity-unchartered-waters-un

Ever since the development of the World Wide Web, it has been unsecure. This is because of its nature, which is that the intention of its creation was for the purpose of helping programmers and scientists. It was never meant to be used to keep government secrets or bank accounts secure. The only reason the majority of users are safe in the World Wide Web is simply because there are more users and data then there are hackers to hack it. When it began in the 1960s, no one expected it to make such a large impact on the world. As it started to gain popularity in the late 1990s and 2000s, especially to individual users, many realized its potential for crime and warfare. Computers were always commonly used in warfare, even in World War I the British used The Colossus, (first operational programmable electronic digital computer) to break German codes. At the time the functionality of this computer was even less the today typical calculator[13].

The first kind of cyber attacks were through malware. The first type of malware that attracted media attention was the Morris Worm. The specialty about a worm is that it spreads by itself, whereas other forms of cyber attacks need to be implanted by a person using some kind of program. The Morris Worm was released by Robert Morris who attended Cornell University, inflicting roughly $10 - $100 million USD worth of damages and infecting nearly 10% of all computers connected to the internet at that time. It showed the world what potential malware had in a cyberattack or cyber warfare[14] setting.

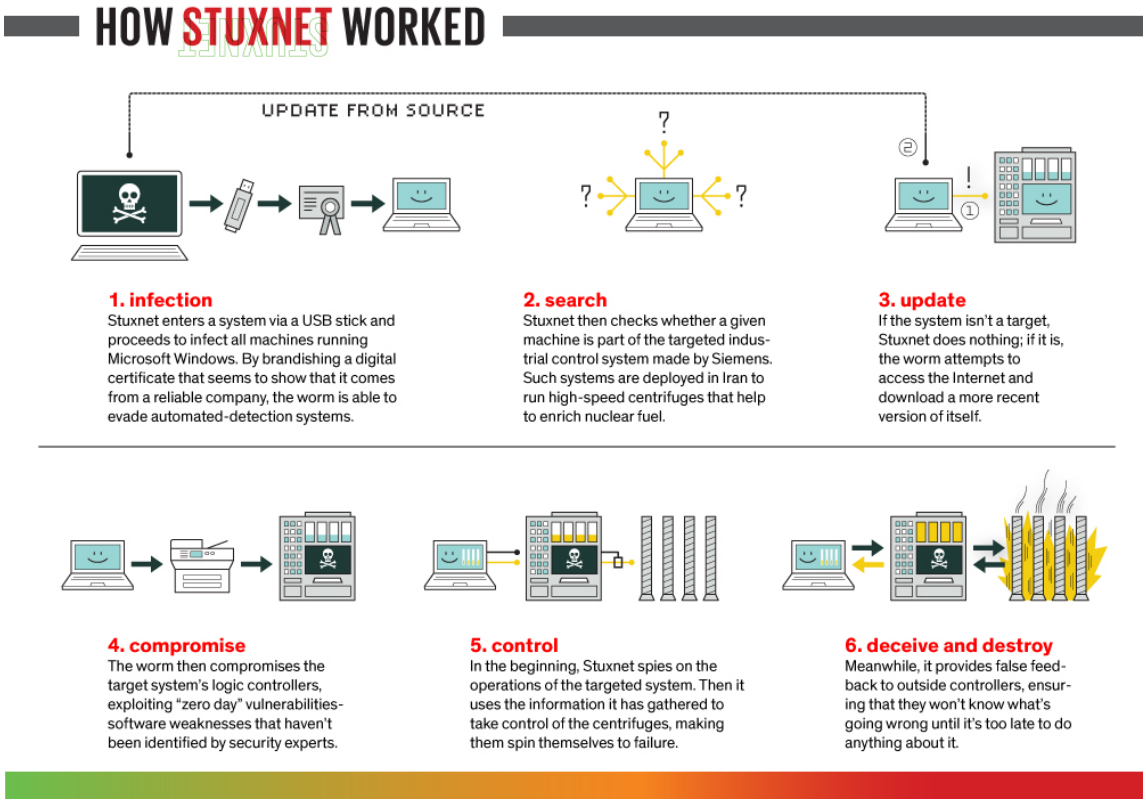
At the time the only use for malware was for profit, what was usually achieved through forced advertising[15]. Since the year of 2003 most of the viruses and worms used in cyberattacks are meant to take full control of a computer to use for additional cyberattacks. These computers are called "zombie computers" and are used for spam, Distributed Denial of Services (DDoS) attacks, phisher scams, viruses, download pornography, and to steal information[16].

One of the major attacks took place against Estonia in 2007. The government websites were hacked by DDoS attacks and were compromised for 22 days. This is particularly frightening because the Russian government is believed to be behind it. This event brings a bit of cyber warfare potential to light, and is the only the start of national cyber attacks. It also shows that it is easy to stay anonymous through the Web, as Estonia was unable to properly prove that Russia was behind the attacks, and so the perpetrator is unknown for certain[17].

---

[13] http://www.historyofinformation.com/index.php?era=1940&category=
[14] http://www.intelfreepress.com/news/lessons-from-the-first-computer-virus-the-morris-worm/7223/
[15]http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_exec_summary_internet_security_threat_report_xiii_04-2008.en-us.pdf
[16] http://www.pcworld.com/article/116841/article.html
[17] Ibid

Another major event was the discovery of Stuxnet in 2010. This was a major that can be illustrated through the visual. The attacks are believed to be run by the USA and Israel, but proof is yet to be shown.



Stuxnet and how it worked - Figure 1.0

The widespread use and development of technology is giving security a run for its money. While the usefulness and efficiency was unimaginable a couple of years ago, this major tool is also a major threat. Cyber-attacks and cyber warfare has the potential to permanently cripple the human race and the whole planet with it. It has also become the new way to commit crimes as there are so many advantages over committing any other type of crime.

First of all, the attacker risks significantly less in cyberspace because of the use of vulnerable off-the-shelf technologies, the challenges of actually tracing the attack back to an attacker, and the hardship of perceiving the difference between glitch and a malicious action. Stuxnet was one of the main reasons national cyber security began being developed and strengthened. The idea of cyber exploitation to become physically destructive and politically motivated was beyond any country's dreams at that time. To this day it is still the only known phenomenon of its kind, to successfully exploit cyberspace to target an industrial process for a destructive goal, while no military confrontation is involved[18].

Apart from some minor crimes and scrimmages, cyberwar has never seen its full potential, and a state sponsored coordinated cyberattack has yet to be seen. The definition and ethical code of conduct for cyberwar has yet to be determined. This leads to many possibilities and requires quick action on the part of the international community[19].

Societies in both past and present have consistently used a two-pronged strategy to maintain the order needed to survive and prosper. This was first by maintaining internal order by defining and enforcing a set of rules which discourage the members of a society from turning on each other in ways that defy order, such as laws. They then maintain external order by complying on military force and agreements from other societies. Now with the possibility of cybercrime and cyber technology this two pronged strategy becomes completely useless and irrelevant. This way of preserving order relies on nations and countries being territorially defined so that societies and distinguishable. Now that cyber criminals can attack from virtually anywhere in the world, attacks can no longer be formatted into an internal-external form and a new form of preserving order must be put in place[20].

Cyberterrorism in its current state is usually meant to demoralize a population by destroying its cyber and physical infrastructure. Because of this and reasons mentioned previously, the international community should and must cooperate to reduce the potential destruction of a cyberattack[21].

---

[18] http://www.cybersecurity-review.com/articles/the-current-state-of-cyber-warfare
[19] http://docplayer.net/17880512-At-light-speed-attribution-and-response-to-cybercrime-terrorism-warfare.html
[20] ibid
[21] ibid

As of this moment, no existing UN document addresses cyber war specifically. Nonetheless, various bodies in the UN are beginning to attempt to regulate cyber warfare. Secretary General Ban Ki-Moon advised the Advisory Board on Disarmament Affairs to pay more attention to cyber warfare in 2009[22]. Ban Ki-Moon noted that the board needs to consider cyber warfare and its impact on international security for both public and private sectors[23].

In 2010, DISEC issued a press release[24]covering a recent debate on potential cyber warfare. In it the Brazilian delegate stated "Modern society's emerging dependence on of the new cutting-edge information and communication technologies was giving rise to new vulnerabilities that could undermine activities of governments, markets, and other entities." It was also mentioned that the international community should establish instruments to deal with cyberwarfare[25]. The report recommended DISEC to deal with criminal activities involving information and communication technologies[26]. It mentioned as well that cyberwar discussions should be all held under United Nations leadership and that the UN should take leadership in qualifying national instruments in terms of cybersecurity, ensuring that no discriminatory policies could prevent access of some countries to technologies involving information and communication[27].

In February 2013 the UN Comprehensive Study on Cyber Crime took place. An intergovernmental expert group conducted the study and it includes the study of the problem, responses to it by member states, and the exchange of information on national legislation, best practices, technical assistance, and international cooperation[28]. The study finds that in the future in such a hyper-connected society, it will become almost impossible for any sort of crime that will not involve electronic evidence linked with the Internet. Adapting to this will require many fundamental changes in international cooperation on criminal matters mechanisms, law enforcement laws, and evidence gathering processes.

The key findings of the study are mostly concerned about issues surrounding fragmentation at the international level, diversity of national cybercrime laws, formal international cooperation in criminal matters through cybercrime, the role of evidence 'location', national legal frameworks, law enforcement and criminal justice, and cybercrime prevention activities[29]. In June 2013, a panel discussion on cybersecurity took place in Germany. Over 130 people from 50 different countries attended and it was titled "Cybersecurity: unchartered waters for the UN[30]." Little was discussed other than the realization of cybersecurity as a real need in our current day society. It strongly emphasizes the need for the implementation of better protection[31].

---

[22] http://www.un.org/press/en/2009/sgsm12108.doc.htm
[23] ibid
[24] http://www.un.org/press/en/2010/gadis3419.doc.htm
[25] ibid
[26] ibid
[27] ibid
[28]https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf
[29] ibid
[30] https://www.eastwest.ngo/events/cybersecurity-unchartered-waters-un
[31] ibid

Because of the lack of discussion and knowledge in the regard of cyber warfare to the international community, there are two main methods of approach. It could either be treated like an extension of our current conventional war, with treaties governing its application. It could also be deemed too risky and too unpredictable to be applied to government, military, or even non-governmental applications[32].

If it was treated like an extension of current conventional warfare it would turn our typical definition of warfare into a new hybrid war system relying on both cyberspace and reality to achieve the results wanted. If this is the case, then the international community and delegates should attempt to compose a treaty that regulates cyber warfare[33]. Like any other sort of warfare it should be used to regulate this sort of warfare and the consequences it produces. International law and its morals should be put into place and decided upon by the international community. There are many difficulties that the delegates will have to work through though, such as the fact that cyberwar is very different from conventional war. Some delegates might not believe it to be able to coexistent in one war at the same time. A good example could be a mention in the Charter of the United Nations which states that a country is allowed to defend itself in the event that it considers itself victim of an act of war[34].

Cyberattacks can be vast and numerous, targeting many areas in different nation states at a time. It is a possibility that your country might be a victim to an act of cyberwar at any given moment. This would in turn make it legal and legitimate for that country to defend itself in full force in either cyberspace or military. There would also be an increase in warfare across the world as cyberwar is much less risky for a country to entail as it would be easier and would require little to no movement of troops. Internet security companies report that at least 130 countries have information warfare programs completed or under development[35]. This international community must avoid the possibility of more warfare under any circumstances.

Cyber warfare can prove to be extremely crippling to a victim country, so delegates could also consider a treaty alike the Nuclear Non-Proliferation Treaty (NPT). While the consequences of cyberwar may not be as evident it is very possible for a country to be completely destroyed through cyberwar. Bank systems and important infrastructure could be damaged greatly, along with the possibility of weapons systems being hijacked. Civilian and government information could be taken into enemy's hands and could be devastating to the country. The reliance on internet can be easily taken advantage of so a treaty might be in the best interest of the delegates[36].

The difference and difficulties of creating a similar treaty is also very prominent. The difference between nuclear devices in war and cyberwar is that cyberwar is easily accessible and readily available for any state or individual. Any sort of non-proliferation treaty will not be as effective unless modifications were made to the treaty. These modifications that can prevent such issues are up to the delegates decisions[37].

[32] https://aiskharvardmun.wikispaces.com/file/view/DISEC.pdf
[33] ibid
[34] http://www.un.org/en/charter-united-nations/
[35] http://law.emory.edu/eilr/_documents/volumes/29/3/Article/jensen.pdf
[36] ibid
[37] ibid

The current ambiguity of cyber warfare in terms of simple research and international law makes it free for states to pursue cyber attacks as another weapon to be used. It is also true that no country wishes to be the victim of such an attack, which makes the bloc positions most interesting.

Countries with Military Based Cyber Warfare Programs

This section includes all states with state-sponsored cyberwar programs for governmental use. Countries that fall in are the majority of the developed world with reliance on internet. The P5, a majority of Western Europe's, and some developed parts of Asia are included in this bloc. These countries typically wish to continue developing their cyberwar systems in order to defend themselves against any cyber attacks as well as to perform espionage on enemy states. They look for methods to combat nongovernmental organizations using cyberattacks and finding the source of such attacks and are intent on developing said technologies. They look to defend themselves against cyber attacks on private and governmental institutions. These nations also look to accomplish the manipulation of important information to deceive the population for propaganda, campaigns, preserving diplomacy, subversion, or deception of local media. They also look to go on the offense against enemy states if needed in terms of cyberwar[38].

Countries with Developing Cyber Warfare Programs

Most countries in this section are in the developing world including most of South America, some of Western and Eastern Europe, some of the Middle East, and Southeast Asia. The programs being developed are limited in size and funding, but provide the bare necessities to ensure that networks are secure. They often lack the financial and technical resources needed to ensure that they stay safe against large scale cyberattacks. These states look to gain assistance from other countries in funding and training of cyber operations or to even simply provide cyber operations in order to protect themselves and not even bother with cyber weapons to attack other countries.

Countries Unable to Pursue a Cyberwarfare Program

Some nations do not have the resources to develop cyberwar programs of any kind. They often rely on others for cyber defense and security. These countries often have political, economic, or social problems preventing them from having a dedicated cyber war program. This group of countries has the most to gain from the complete banning of cyberwar. They simple do not have the resources to keep up with the rest of the world with cyberwar technology and would certainly be hurt if any person or nation decided to attack them through cyberspace. They also benefit from the strong regulation of cyber warfare. For this bloc is absolutely vital in creating an international treaty or resolution that addresses the use of cyberwar.

[38] ibid

1. What would be most vital in establishing war morals for cyberwarfare?
2. Why would nation states or individuals be motivated to commit a cyber attack and what would motivate them the most?
3. How can we keep the public safe from personal attacks through cyberspace?
4. What parts or details of countries would most likely be attacked through cyberspace?
5. How could cyberwar be fitted into our current conventional warfare?
6. How could we achieve and enforce the banning of cyberwar internationally if needed?
7. How can we ensure and enforce cyber weapons so that they are only used under international law?

To assist in your research please feel free to utilize the sources provided.
http://docplayer.net/17880512-At-light-speed-attribution-and-response-to-cybercrime-terrorism-warfare.html

https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

http://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf

https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf

"United Nations, Main Body, Main Organs, General Assembly." UN News Center. UN, n.d. Web. 11 Sept. 2016.

"United Nations, Main Body, Main Organs, General Assembly." UN News Center. UN, n.d. Web. 11 Sept. 2016.

"Chapter IV | United Nations." UN News Center. UN, n.d. Web. 11 Sept. 2016.

"Sixty-sixth Session of the General Assembly." United Nations Association of Slovenia. N.p., n.d. Web. 11 Sept. 2016.

"Internet Live Stats - Internet Usage & Social Media Statistics." Internet Live Stats - Internet Usage & Social Media Statistics. N.p., n.d. Web. 11 Sept. 2016.

Karlgaard, Rich. "Internet Guru: Google Evangelist Vint Cerf." Forbes. Forbes Magazine, n.d. Web. 11 Sept. 2016.

"Cyber Warfare, Unchecked, Could Topple Entire Edifice of International Security, Says Speaker in First Committee at Conclusion of Thematic Debate Segment." United Nations. United Nations, n.d. Web. 11 Sept. 2016.

"Cyberwar Timeline." Infoplease. Infoplease, n.d. Web. 11 Sept. 2016.

Comprehensive Study on Cybercrime. New York: United Nations, 2013. Web. 11 Sept. 2016.

"Cybersecurity: Unchartered Waters for the UN | EastWest Institute." Cybersecurity: Unchartered Waters for the UN | EastWest Institute. N.p., n.d. Web. 11 Sept. 2016.

"Timeline Outline ViewEra: 1940 - 1950 | Theme: All Themes." Timeline Outline View : HistoryofInformation.com. N.p., n.d. Web. 11 Sept. 2016.

@intelfreepress. "Lessons from the First Computer Virus: The Morris Worm." Intel Free Press. N.p., 20 Feb. 2014. Web. 11 Sept. 2016.

Internet Security Threat Report 2014. Mountain View, CA: Symantec, 2014. Web.
/.latest_citation_text

"Zombie PCs: Silent, Growing Threat." PCWorld. N.p., 09 July 2004. Web. 11 Sept. 2016.
By Lior Tabansky, Cyber Security Policy Expert, Tel Aviv University, the Yuval Ne'eman Workshop for Science, Technology and Security. "Cyber Security Review." Cyber Security Review. N.p., n.d. Web. 11 Sept. 2016.

By Claiming Responsibility for the Catastrophe, the Cyberterrorists It Is Not Merely a Possibility, but an Inevitability. See, E.g., Arquilla, Waging War Through the Internet, Supra Note 38, at El. Despite... Al Qaeda's Long-standing Interest in Cyber Ter. "At Light Speed: Attribution and Response to Cybercrime/Terrorism/Warfare." ⋆. N.p., n.d. Web. 11 Sept. 2016.

"PAY MORE ATTENTION TO CYBERWARFARE, VERIFICATION, SECRETARY-GENERAL ADVISES IN REMARKS TO ADVISORY BOARD ON DISARMAMENT AFFAIRS." United Nations. United Nations, n.d. Web. 11 Sept. 2016.