Cybersecurity

Topic Background

The growth of the Internet has allowed nations, organizations, and people to connect in ways previously unimagined. This new interconnectivity has allowed for collaboration, partnerships, and growth to reach unprecedented levels and has permitted the world to become a much smaller place. However, along with the benefits of the Internet, there are many new dangers created by this technology. The very nature of the Internet allows for individuals to hack information systems to steal information, cripple the delivery of services, and commit fraud. These cybercrimes are difficult to fight against, so it takes an international effort to combat them.

This issue has come to the forefront in recent months after it came to light that the Chinese government was responsible for a series of hacks against American government offices and businesses. In 2015, the United States Office of Personnel Management was hacked which resulted in over 20 million government employees' sensitive information being leaked to members of the Chinese government. In recent years, numerous hacks against American businesses have also been identified. The objective of these hacks has been to steal industrial secrets. This has angered American businesses because they have spent millions of dollars to develop new technologies and now Chinese businesses can have them for free.

Sometimes cyberattacks can have more tangible effects. In 2009, the US and Israel launched the Stuxnet virus against Iranian nuclear enrichment facilities and were able to to destroy roughly a fifth of all of their centrifuges by making them spin out of control.[1] In 2007, Estonia was targeted by Russian sympathizers for wanting to remove a Soviet statue from the capital, Tallinn. Several prominent government websites were hacked, and essential government services were disrupted.[2] In December 2013. the credit and debit card information was stolen from over 40 million shoppers at Target stores over the holiday season. After it was announced, people avoided shopping at Target and the company lost 46% of its profits and had to pay over $10 million in damages to affected shoppers.[3]

Some analysts warn this is only the beginning. As the internet and internet-linked technology become more widespread, the potential danger of cybercrimes increases. If nothing is done to combat this scourge, almost nothing can be considered safe. Smartphones could provide hackers with a wealth of financial and other private information from its users. Stock markets could be

[1] "Stuxnet was Far More Dangerous." Business Insider. http://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11
[2] "Denial-of-Service." International Affairs Review. http://www.iar-gwu.org/node/65
[3] "9 Recent Cyberattacks Against Big Businesses." The New York Times. http://www.nytimes.com/interactive/2015/02/05/technology/recent-cyberattacks.html

manipulated to wipe out entire economies overnight. Power plants and water treatment facilities could be switched off, leaving people without basic necessities. Clearly this is an issue which needs to be addressed and the only way to address it is through international dialogue and cooperation.

Past Actions

The UN General Assembly, Economic and Social Council, and Security Council often stress the importance of cybersecurity and regularly call on member nations to combat cybercrimes. These organs usually refer responsibilities to the International Telecommunications Union (ITU) which is a UN agency based in Geneva which is responsible for coordinating efforts on these issues. They study cyber activity and set standards to which various governments are supposed to adhere to.[4] The difficulty with such organizations is these standards are often non-binding and there are not enough mechanisms to force countries to play by the rules.

A major difficulty in combating cybercrimes is the sheer amount of data that needs to be monitored in order to catch cybercriminals. Several NGOs have stepped up efforts to monitor cyber activities and on reporting on cybersecurity issues. The International Association of Cybercrime Prevention, "provides information and training about cybercrime prevention. It is also an interdisciplinary research organization bringing together experts, professionals, and individuals involved with the misuse of Information Communications Technology."[5] The Cyber Peace Foundation is another NGO which is also involved with raising "awareness, counseling, education, training and to reach out to the citizens, the governments, law enforcement agencies (LEAs), private enterprises, NGOs working in cyber crimes and cyber security, universities, cyber security experts and bug bounty hunters; to provide a common platform on a global level."[6]

There is also hope that bilateral agreements can help solve these issues. In September 2015, Chinese President Xi Jinping and American President Barack Obama met and discussed issues related to cybersecurity and came to a tentative agreement. Prior to President Xi's visit to Washington, Obama administration officials had warned that Chinese companies which had benefited from stolen information might be sanctioned by the US government, and their products might not be able to be sold on international markets. In their meetings, they discussed steps each government should take to curb cyber-spying and they agreed to stop allowing their governments to commit economic espionage on each other's native companies.

---

[4] "About ITU." International Telecommunications Union. http://www.itu.int/en/about/Pages/default.aspx
[5] "About Us." International Association of Cybercrime Prevention." http://www.cybercrime-en.org/about-us-cyber-crimes
[6] "About Us." Cyber Peace Corps. http://www.cyberpeacefoundation.org/aboutus.html

Possible Solutions

It is important for delegates to keep the following in mind when brainstorming solutions to cybersecurity threats:

1. What measures can be taken to improve the monitoring of cyberspace?
2. How can international actors be held accountable when they are found to have taken part in cybercrimes?
3. What steps can be taken to ensure a free, but safe Internet?

One of the major problems with guaranteeing cybersecurity is the sheer amount of data that makes up cyberspace and, coincidentally, the difficulty in monitoring it all. The United States has been better able to monitor cyberspace than many other nations, but this has created some difficulties within the international system. Some nations have viewed America as the greatest protector of cyberspace while others view it as its greatest threat. Increasingly, individuals have become more worried about privacy issues and leaks of government information from Edward Snowden have only increased this worry. Also, since most of the servers which contain the Internet reside within the United States, there is concern that the US has an unfair monopoly in cyberspace ownership. Increasingly, it has been argued that the Internet needs to be governed by an international agency which is responsible to answering to the international system as a whole and not individual parties. The makeup of such a body is still being debated.

Another major problem with guaranteeing cybersecurity is the issue concerning how to hold nations and international actors accountable for their actions. Nations like Russia and China believe cyberspace should be controlled locally by various national governments and should promote national policy agendas. In the West, people believe in a free Internet, but in authoritarian countries like Russia and China, leaders feel threatened by a free internet and wish to control it directly.

Coincidentally, this has sparked debate around the world about how much freedom individuals are willing to give up in order to maintain security online. Originally, the Internet was a completely free place where individuals could express themselves and feel free to come up with applications never thought of before. As the technology has become more widespread and available, dangers have arisen. There is a large debate concerning how much freedom should be allowed in cyberspace. If governments took more control over cyberspace, they could most assuredy be more effective in improving cybersecurity, but there is a risk they would also decrease the level of freedom permissible on the Internet. This debate is especially pertinent in the European Union where individuals are asking where to draw the line between security and freedom of expression.

There are many challenges to creating an international framework for cybersecurity. Though the challenges are great, the potential danger of not doing anything is far greater. The problems posed by cybercrime are serious, but they are solvable. It is hoped the international community can put aside their differences and create a free and open Internet which is safe from cybercrime.

Further Research

- The UN and Cybersecurity
- Information on International Telecommunications Union
- Information on Cyber Peace Foundation
- The Cyber Security Forum Initiative

Questions

1. What was the name of the virus the United States and Israel launched against Iran?
2. What store was targeted in December 2013 to obtain users' credit/debit card information?
3. What was the name of the office which was targeted by the Chinese government in 2015 to steal federal employees' information?
4. Who met in September 2015 to work out disagreements concerning cybersecurity?
5. Which country is often thought of as the greatest protector of and greatest threat to cybersecurity?

Answers

1. Stuxnet
2. Target
3. The Office of Personnel Management
4. Chinese President Xi Jinping and American President Barack Obama
5. United States of America