Baltimore Area Training Model United Nations Conference 2019

Background Guide: Threats to Cybersecurity

Introduction

Why Is Cybersecurity Important?

The topic of Cybersecurity has already gained an enormous amount of significance, and as technology continues to race forward, so does the importance of a globally secure cyber network. Cyberspace is an asset in connecting the international community. However, the more connected countries – and the people in them – become, the easier it becomes to target large groups of people and large blocks of countries simultaneously. It has even been noted by previous UN assemblies that if cyber warfare goes unchecked it could "topple [the] entire edifice of international security." 1

Cybercrimes fall into two broad categories that are detrimental to the stability of the international cyber community: data breaches and sabotage.2 Data breaches are a risk for everyone from the common person to international organizations, as these can come in the form of stealing personal identification information to state secrets. Often these breaches occur to steal money in some form or another, and it has been estimated that cyberattacks "cost the global economy over $400 billion per year."3 Sabotage, on the other hand, can be in many forms but generally aims to disable systems for whatever purpose. The real threat of these attacks lies in that most cyberattacks go unnoticed until it is too late, if they are ever noticed at all.

Currently, while there have been discussions regarding the necessity of combating and preventing cyberattacks, there is no singular, international effort to bolster cybersecurity. It is imperative that a united effort is decided upon, as all countries need to be held to certain standards not only to combat attacks, but to prevent more from occurring in the future.

Major Issues the Committee Must Address

There are several major issues that must be addressed in order to combat the existing and future threats to cybersecurity. First, there is the issue of transparency. The UN has spent its history creating a cooperative international community. As means of attack advance, it is important that cooperation efforts advance as well. The issue of transparency is directly tied into the need for some measure of checks and balances on UN members, which must be addressed by the Committee as well. Second, threats as they have previously been identified must be addressed. As previously stated, cybercrimes broadly fall into two categories: data breach and sabotage. These attacks can be further divided into identified categories of cybercrime, cyber espionage, cyber terrorism, and cyber war. To fully understand these categories, definitions have been provided:

1. Cybercrime is "the use of computers or related systems to steal or compromise confidential information for criminal purposes, most often for financial gain," 2. Cyber espionage is "the use of computers or related systems to collect intelligence to enable certain operations," 3. Cyber terrorism is "the use of computers or related systems to create fear or panic in a society," and

1. October 2014, https://www.un.org/press/en/2014/gadis3512.doc.htm.
2. 2 Detlev Gabel, "Cyber risk: Why cyber security is important," White & Case, 1 July 2015, accessed 1 July 2017.
3. 3 Ibid. 4 Harry, Katzan, Jr., "Contemporary Issues in Cybersecurity," Journal of Cybersecurity Research, June 2016, accessed 1 June 2017.

2. Cyber war "consists of military operations with cyberspace to deny an adversary. . . the effective use of information systems and weapons." 4 Please note, that while these definitions are widely used, they have not been agreed upon by the UN member states and variation in the definitions across states allows for the acceptance different activities. A main goal of this Committee is to create a feasible way to combat these cyber attacks, if not to stop them altogether.

It is also imperative that the Committee address ways to deal with emerging threats. Technology advances at an incredibly fast pace, and so it is necessary to stay up-to-date with combatting new types of attacks as soon as possible once they have emerged. Additionally, the platforms that are at risk and thus necessary to be included in cybersecurity needs to be discussed.

Historical Background

Notable Past Cybersecurity Threats

The Morris Worm

In 1988, Robert Tappan Morris created the first computer worm ever to be transmitted through the internet, aiming not to harm but to determine exactly how vast cyberspace is.5 Unfortunately, the worm mutated and ended up infecting over 600 computers in an estimated $100 million dollars of damage.6 While it may have been unintentional, this denial of service to those computers via the Morris Worm is the first documented case of cyber sabotage and has inspired many contemporary attacks.

Solar Sunrise

Ten years after the Morris Worm, in what was originally thought to have been an Iraqi effort to seize US government and private computer systems, over 500 systems running on the Sun Solaris operating software were seized by the hackers.7 The culprits were later found to not be Iraqi operatives, but rather three teenagers from California. While this revelation did halt any backlash that may have been caused on the international scale, the attack itself was able to cripple the entire country's software infrastructure. This highlighted exactly how extensive a collaborative effort could be on both the private and public sector, particularly because the attack had been an effort by three rookie hackers.

Teen Hacks NASA and the US Department of Defense

Only one year later, another teen by the name of Jonathan James was able to penetrate both the US Department of Defense and, using the information stolen, he was able to steal part of a NASA software program, shutting down systems for three weeks.8 This event highlights both data breach and sabotage crimes, showing that the two are not mutually exclusive. As the software stolen was also related to the International Space Station, the attack also showed that one crime could affect not just one nation, but many all at once.

5 "Top 10 Most Notorious Cyber Attacks in History," ARN, accessed 1 June 2017.

6 Ibid.

7 Ibid.

8 Ibid.

9 Ibid.

10 David McGuire and Brian Krebs, "Attack On Internet Called Largest Ever," Washington Post, 23 October 2002, accessed 30 July 2017.

11 Ibid.

12 "Top 10," ARN.

Internet Attacked

In 2002, the largest attack on the internet of the time occurred, shutting down the internet for an hour.9 Although the average user was unable to notice any changes in service due to safeguards, the hackers were able to attack and shut down 13 of the main root servers that provide internet. Had the attack lasted for longer, even the average user would have been able to feel the attack. This attack brought this issue to the forefront of global attention. The problems boiled down to money and vulnerability. Experts on the issue stated that the "only way to stop such attacks is to fix the vulnerabilities on the machines . . . There's no defense once the machines are under the attacker's control."10 It was also noted by the same experts that only those with money would even be able to protect themselves, and even then, it would be unlikely that their systems would be able to withstand a concerted attack.11 This attack was a much-needed wake-up call to exactly how vast threats could be and how very little could be done to combat them. Years later, money and vulnerabilities in machines and software are still some of the largest problems in combatting attacks. It also remains a problem that most attacks can only be prevented, and if one is able to be launched, it is much, much more difficult to stop the attacks and can cost the targets millions of dollars, mainly because it would shut down the servers of important banks, stock exchanges, corporations, etc. The ramifications of this attack in regards to information are also vast, as the servers would have been left unguarded, making it that much easier to steal valuable information from individuals, corporations, governments, and international organizations.

Google China hit by Cyber Attack

In 2009, Google China was hit by a cyber attack in which hackers infiltrated Google's corporate servers in order to steal intellectual property – main Gmail accounts owned by Chinese human rights activists.12 This crime was later also found to be tied to unauthorized access to private Gmail accounts of users in the US, China, and all over Europe. China is known to be rather stringent in its internet policies and censorship and this is yet another example of a nation targeting those who are a threat. It also shows that a corporation that is used worldwide is not impenetrable, despite many using it to send and share private information.

July 2009 Cyber Attacks

In a series of coordinated attacks, hackers were able to infiltrate thousands of computers belonging to US and South Korean government agencies, media agencies, and banks. The attacks were done with a botnet, or group of hijacked computers. The assumed aim of the attack was to cause disruption, rather than steal information.13 Despite not having that large of an impact on the computers, if the attack had gone as planned, the estimated cost associated with the websites being down would have been huge, as it would have prevented business transactions from being carried out as planned and halted government work. The troubling aspect of these attacks came from the unknown perpetrator. It was largely assumed by Korean Intelligence agencies that the attack stemmed from North Korea. However, it was also found that the hijacked computers hailed from all over the globe, making it difficult to pinpoint those at fault.

Canadian Government Hacking

In February of 2011, Canadian government officials became aware of a cyber attack being performed by foreign hackers. The IP address of the hackers was traced back to China, and before the attack was noticed, the hackers were able to penetrate three government departments.14 The hackers were able to transmit classified information back to themselves, and in the end, Canada had to cut the internet access off for those departments to stop the transmission of information.15 This further highlighted what had been stated previously, that attacks, once started, are hard to stop.

13 Choe Sang-Hun and John Markoff, "Cyberattacks Jam Government and Commercial Web Sites in U.S. and South Korea," The New York Times, 8 July 2009, accessed 15 June 2017. http://www.nytimes.com/2009/07/09/technology/09cybe r.html

Flame

Noted as one of the "most complex threats ever," Flame was a malware attack targeting countries in the Middle East, including Iran, Israel, Sudan, Syria, Lebanon, Saudi Arabia, and Egypt.16 The malware was suspected of having operated since August 2010, despite it not being discovered until mid-2012, and its origins were hard to trace, like the previous attack on the US and South Korea. The reason it was able to go undetected for so long is that the target of this malware was not to damage the system, but instead to collect massive amounts of sensitive information from over 600 targets, including individuals, businesses, and government institutions.17 Because of the size and sophistication of Flame, experts theorized that it would have to have been a government-backed operation, as the only known organizations to have that kind of software are cyber criminals, hacktivists, and government organizations; when this knowledge was paired with the geographic location of the target states and that the attack was not designed to steal money, the only possible culprit left was a government organization, although which one or ones are still a mystery.18 This attack was far superior to those known prior—rather than just siphoning information existing in cyberspace, Flame was capable of "recording audio via a microphone. . .take screenshots of on-screen activity, [and] automatically detecting when "interesting" programs – such as email or instant messaging – were open."19 Flame showed the world that what preventive and protective measures were in place against known attacks were already too far behind what had been further developed. Flame highlights the need for technologies that counter cyber attacks to advance as quickly as the technologies that perform them. However, it also revealed another issue of how technologies advance is not always easy to predict, and thus is not always easy to guard against.

India Government Hacking

Despite being a technology powerhouse, India was still hit by a large-scale cyber attack, which left the email accounts – and the sensitive information inside them – of over 10,000 government employs compromised.20 The attack seemed to try to obtain specific information, rather than simply disrupt system use or steal funds. In fact, of the information stolen, a large part of was of troop deployment plans, especially of the Indo Tibetan Border Police, whose plans were compromised.21 This attack was a very real example of how the information being stolen could not only affect cyber information, but could have very tangible real-world repercussions that could be detrimental to the safety of many.

#opIsrael

Israel is one of the most contested and volatile regions in the world, and on April 7, 2013, it also became the target of a vicious cyber attack. The coordinated attack, known as #opIsrael, aimed to erase Israel from the internet on the eve of Holocaust Remembrance Day. 22 The attacks targeted both the public and private sector. Because the attacks had been known prior to occurrence because of the use of the hashtag, #opIsrael is widely regarded as a failure. However, it calls into focus the use of social media platforms, which continue to this day to advance and take over the common person's day, to perform cyber crime. It also showed a case of a long-standing fight being taken out of the real world and placed into cyberspace, a trend that continues to grow.

14 Syed Balkhi, "25 Biggest Cyber Attacks in History," List 25, 11 May 2014, accessed 1 June 2017, http://list25.com/25-biggest-cyber-attacks-in-history/.

15 Ibid.

16 Dave Lee, "Flame: Massive cyber-attack discovered, researchers say," BBC News, 28 May 2012, accessed 1 June 2017, http://www.bbc.com/news/technology-18238326.

17 Ibid.

18 Ibid.

19 Ibid. 20 Phil Muncaster, "10,000 Indian government and military emails hacked," The Register, 21 December 2012, accessed 15 June 2017. https://www.theregister.co.uk/2012/12/21/indian_govern ment_email_hacked/ 21 Ibid. 22 Balkhi, "25 Biggest Cyber Attacks."

Contemporary Conditions

In Spring of 2017, two cyber attacks occurred that "the World [wasn't] ready for" in the form of a breach of IDT Corporation23 and the subsequent WannaCry breaches that seized power of English hospital computers, Chinese universities, German railways, Japanese auto plants, and other organizations in over 100 countries.24 While the demands for ransom and the temporary loss of power were devastating enough, it later became apparent that the attack had had a goal other than money in mind: it had also taken the information on the employees of IDT, allowing the hackers access to sensitive information, as well as other sensitive information gained from the hospitals, universities, and other breaches, putting lives at risk both immediately, like those in the hospitals and railways, and in the future.25 Experts claim this is a new type of cyber attack the world simply is not prepared to face, as the attacks are becoming virtually undetectable until it is almost too late, or even until after the point of no return, especially because there is no leading force in securing cyberspace.26

Thus, that leaves cybersecurity as it currently stands today: with technology racing ahead, cybersecurity is scattered and falling increasingly behind. Starting even at the root of the problem, there is not even an agreed upon definition of cybercrime around the world and many countries still feel that it is an IT issue, rather than one of international concern.27 Countries are reluctant at best to show transparency regarding cybersecurity and activities in cyberspace with even the closest of allies; attacks are also developing into hybrids that affect not only cyberspace but are very real dangers in the real world, whether it be in significant financial loss or the loss of lives.

Therefore, despite the fact that "the UN has been trying to implement meaningful guidelines on international cybersecurity for the better part of the last 15 years," no consensus is able to be reached, and all security measures continue to fall further and further behind the unpredictable and virtually undetectable attacks.28

Past UN and International Action

While there has been no consensus or successful hardline defense against cybersecurity on the international stage, there have been several notable efforts to secure cyberspace: 1. UN Resolution 57/239, passed in 2003, called for more awareness of capable nations "to prevent, detect, and respond to cybersecurity threats;" 2. One year later, Resolution 58/199 invited member nations to share cybersecurity strategies with other member nations, as they saw fit.29 While both of these resolutions were optimistic, they did little in creating actual transparency between member nations, as neither were enforced strictly, and cybersecurity threats continue to be among the most notable type of attack of the 21st century. 30

23 United Nations News Centre, In wake of 'WannaCry' attacks, UN cybersecurity expert discusses Internet safety, 19 May 2017. 24 Nicole Perlroth, "A Cyberattack 'the World isn't ready for,'" New York Times, 22 June 2017, accessed 17 June 2017. https://www.nytimes.com/2017/06/22/technology/ransomw are-attack-nsa-cyberweapons.html 25 Ibid.

26 Ibid. 27 UN News Centre, 17 May 2009. 28 Michael Beaver, The United Nations and Cyber Warfare, Global Risk Advisors, 28 September 2016, accessed 20 June 2017. https://globalriskadvisors.com/blog/united-nations- cyber-warfare/ 29 Ibid. 30 Ibid.

Questions a Resolution Must Answer

1. What, by definition, is considered a cybercrime?

Before it can be determined how to prevent cybercrime, a universal definition is needed. Without one, all countries will not be held to the same standards and will not be targeting the same activity, thus making any combined efforts against cybercrime inefficient.

2. How is cyber warfare going to be defined from this day forward?

Similarly to cybercrime, cyber warfare also needs a universally, acknowledged definition that distinguishes it from cybercrime. This is necessary as cyber warfare is often more extreme and will warrant a more severe punishment, and a line needs to be drawn between the two types of attacks.

3. Is an act by a non-governmental individual against another nation's organization considered an act by the state or by the individual?

While the aggressor will be dealt with regardless, it is a matter of international peace whether or not an individual acting without government consent is considered a state act or not. Without this acknowledged, every attack by an individual can be used as a reason to retaliate against an entire state, which may have had no responsibility for it in the first place.

4. What measures will be taken in the event of a cybercrime against the aggressor?

In order to dissuade aggressors from attacking in the first place and to punish those who still decide to attack, the appropriate repercussions need to be in place. Ideally, several measures of varying degrees of severity, as in normal crimes, so that the punishment may fit the crime.

5. What type of preventive measures need to be taken?

One of the biggest problems with cybersecurity is that it is developing at a much slower rate than the technology being used to attack. Some sort of committee or similar organization needs to be set up in order to keep up to date with the attacks and develop the preventive measures as quickly as possible. Ideally, this organization would reach a point that it is able to predict the next step in attacks advancing and be proactive, rather than continually stay a reactive measure.

6. What parameters need to be set to decide what platforms need to be included in cybersecurity?

Cyberspace is a large place, encompassing many different types of information, media, and other various things. In order to protect and defend accurately, the different parts of cyberspace need to be assessed for risk and then decided which ones are covered by cybersecurity and to what degree.

7. In addition to cybersecurity encompassing the world wide web, what social media platforms will it cover?

Social media platforms are a growing way that information about persons is accessed. It needs to be decided which, if any, of the social media platforms fall under cybersecurity.

8. In what legal and transparent ways will the dark web be covered by the measures against cybercrime?

Cyberspace does not just include the platforms used by the everyday person. Rather, many crimes begin on the dark web, where trading of information and tangible goods is done illegally. The dark web is harder to monitor, however, so it necessary to create measures regarding the legality of this as well.

Bloc Positions

United States and Developed Nations

The US has been the target of the many of the attacks in cyberspace. As one of the leaders of the world, it has

made a habit of condemning the attacks and under the Obama administration, began making more concerted efforts to reach international cooperation.31 Currently, the US is trying to create an international community willing to share in transparency and defense efforts. At the same time, the US also aims to build a tech savvy workforce that is able to spot and defend against attacks when necessary. The US acknowledges that "the economic prosperity, national security, and personal liberties depend on [its] commitment to securing cyberspace and maintaining an open, interoperable, secure, and reliable Internet."32 Similarly, developed nations in both Europe, the British Commonwealth, and Asian countries, like South Korea and Japan, among other nations, have had similar experiences with cyber attacks and tend to hold similar views to the US in terms of securing cyberspace.

China

China has been a target of much criticism for its harsh and restrictive policies regarding cyberspace for its citizens, and because of the fact it was one of the last developed world leaders to release its cybersecurity plan.33 The plan that China did eventually release, articulated plans to overcome the digital gap, digital economy, and cybersecurity, among other issues. However, the Chinese plan must be heavily scrutinized in regards to its discourse with Chinese internet policy. China has also been found as both a victim and a perpetrator of cyber attacks over the years, both on its own citizens and allies and on its biggest competitors. However, in its recent moves to address cyberspace, China is opening up space so that it may build trust with the US and other countries in hopes of building a cyber community that they, too, are included in.

Russia

Russia is another country that has been both a victim and, often, a perpetrator in cyber attacks. Notably, there was the recent scandal of whether or not Russia had hacked into the US election to choose the outcome they felt would be most favorable for them. Their views as a whole differ entirely from the Western point of view. While most Western countries acknowledge a need for a certain degree of transparency, Russia believes that all cyber information should be accessible and does not think that physical borders exist in cyberspace, thus taking information from those they see fit.34 Russia continually tries to submit proposals along these ideals and to normalize their viewpoint, which has made it difficult to come to agreements with Western countries and those of the same viewpoint.

North Korea

While North Korea has not issued an official statement on their position regarding cybersecurity, it is of concern to many nations. North Korea has begun moving more and more to cyberattacks, which are unpredictable and difficult to detect, making them even more dangerous. The greater North Korea's cyber capabilities, the bigger of a threat they become, which leaves its opposition even more on edge and wishing to reach an agreement.

Underdeveloped and Developing Nations

While cybersecurity is not the biggest of concerns to nations whose access to such platforms is limited, it is important these countries are included in the planning of such structures. They also should be included in participating in the structures that are set in place as to have more of a chance to get involved in cybersecurity.

31 The White House, "Foreign Policy: Cybersecurity". accessed 1 August 2017 32 Ibid.

33 Lu Chuanying, China's Emerging Cyberspace Strategy, The Diplomat, 24 May 2016, accessed 1 August 2017

34 Kier Giles, Russia's Public Stance on Cyberspace Issues, Conflict Studies Research Center, 2012., accessed 2 August 2017.

Middle East

Like most other countries, those of the Middle East have been both victim and perpetrator in cyberattacks. The target in the Middle East tends to arise from the lucrative businesses in the area, such as the oil industry, as well as the unrest that plagues the area. Despite many of the countries attempting to bolster cybersecurity, the tensions in the area, which involves many more countries than just those in the Middle East, have made cybersecurity a goal of utmost importance. However, as the countries have a history of clashing against each other and a history of bad blood, it is going to be difficult to achieve levels of transparency between these countries, who are going to be eager to hear what their opposition will say, but want to keep their secrets hidden.

Conclusion

Cybersecurity has emerged as one of the most important issues in the 21st century, while still managing to be one of the most underdeveloped areas of defense. Like, security in real time, it is important that states are able to identify and stop attacks, or even prevent them altogether. However, as technologies advance much more quickly than plans of defense, many attacks go unnoticed until it is entirely too late.

In order to secure one of the most important platforms of information storage and communication, several big issues need to be addressed, including transparency between states, defense, and preventive measures. While there have been efforts by smaller groups of states, there needs to be a general consensus carried forth by member nations, so as to finally stand a chance against the issue.