ODUMUNC 39

Disarmament and International Security Committee

The Future of Cyber Intelligence

By: Joseph Espinoza

ODUMUNC 2016
Issue Brief for the GA First Committee

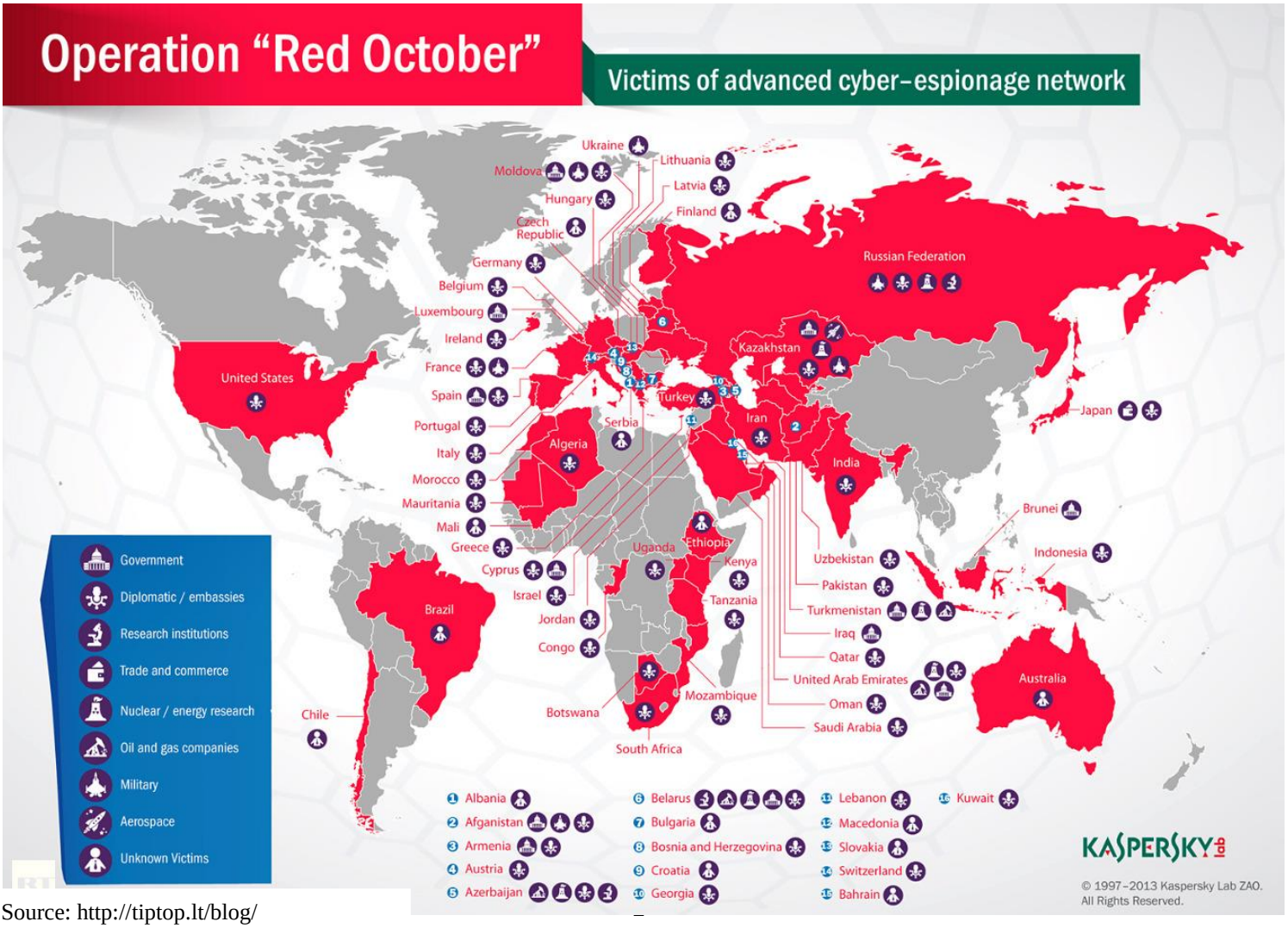
The Future of Cyber Intelligence

By: Joseph Espinoza
Old Dominion University Model United Nations Society

Introduction:

In 2014, a security report showed that, on average in the United States, a new and unknown malware variant was being downloaded to company networks every 27 minutes with a new both infecting the network every 24 hours. The viruses and malware that were uploaded into servers had the potential to steal credit card information and other personal information, or simply deny users service. This is just a sliver of evidence that proves that cyber intelligence gathering is, by far, one of the most effective means of collecting data, crippling economies, and, in some cases, destroying entire nuclear programs, all from the comfort of your own home. Each state has their distinct branch of a cyber security division.

Whether it is called computer security, cyber security, or IT security, the major three goals for any group is to provide, governments, military branches,



Source: http://tiptop.lt/blog/

By: Joseph Espinoza
Old Dominion University Model United Nations Society

corporations, financial institutions, hospitals, and other businesses to collect process and store confidential information on computers. These computers, being on a secure network, would be able to transmit this information to other computers. With the ever-growing increase and sophistication of cyber-attacks, constant and ongoing attention is required to protect this sensitive information as well as to protect national interests and security.

The question, however, isn't *why* a person, or group, steals information and it isn't about what they are going to do with the information they stole. The questions most ask are "How did they do it?" and "What did they get?" In an era where cyber-attacks and digital spying are the top threat to national security and eclipsing terrorism, and where you can tweet @ the American Army, how will the international community handle the use cyber security? More importantly, what is the role of allies in the world of cyber security? Is there such a thing?

What is Cyber Security?

Cyber security has two distinct definitions. The definitions of cyber security are:

1) The protection of information systems from theft or damage to the hardware, the software, and to the information on them, as well as the disruption or misdirection of the services they provide.

2) The product resulting from the collection, processing, integration, evaluation, analysis, and interpretation of available information concerning foreign states, hostile or potentially hostile forces or elements, or areas of actual or potential operations; the activities that result in the product; the organizations engage in such activities.

Although one is much more technical, both definitions convey the same basic idea. The purpose of cyber intelligence is to collect, analyze, and process data in order to make targeted decisions that will benefit the user, whether in business or military practices. The action of also defending your own networks typically falls under the branch of cyber security.

Under the umbrella of cyber security, there is a branch titled cyber-data collection. This is closely related to cyber security, seeing as this is where data is not only collected, but also processed in a repetitive manner. In order to appropriately ascertain what is needed, most corporations begin with planning and direction to determine what the initial target for cyber gathering is. Step two, which happens to be the lengthiest and most continuous step, is the actual gathering of intelligence. The way gathering occurs is dependent on the intelligence needs itself. Once the information has been gathered, the information is then processed into something that can be used to become a product. A product tends to be how you will address the situation with all given information and variables. A product is, essentially, how you will "fix" the problem. The last step is the dissemination of the

The Future of Cyber Intelligence

By: Joseph Espinoza
Old Dominion University Model United Nations Society

product and of the intelligence itself. The information can be used during meetings in order to refine the product if it fails to meet its intended goal.

The Problems of Data Collection

The Roman poet Juvenal in his work *Satires*, stated "*Quis custodiet ipsos custodies*?" (Who will guard the guards themselves?). This theme can be found throughout modern society as well, even popular television shows like *Star Trek the Next Generation* with episodes like "Who Watches the Watchmen" bring to life the same basic question posed almost two thousand years ago. The modern version of this question is infinitely more complex, and one of the sectors of this issue of oversight is cyber intelligence gathering.

The most well-known data collection scandal to occur in the past five years is the case that happened in the United States with Edward Snowden and the National Security Agency (NSA). In May of 2013, Edward Snowden, a former contractor, stated that the United States National Security Agency was collecting the telephone records of tens of millions of Americans. Upon further investigation, it was revealed that NSA had been tapped directly into the servers of nine Internet firms, which included Google, Microsoft, and Facebook. The name of the surveillance program was named Prism. Although there were waves of public backlash, both at the NSA for conducting the cyber surveillance and at Facebook for allowing the NSA to allow it to happen, this wasn't something that was ground breaking and new; it had occurred before, but only under a different name. In the United States, the cyber surveillance program before Prism

NSA Whistleblower Edward Snowden
Image Source:
http://america.aljazeera.com/articles/multimedia/timeline-edward-snowden-revelations.html

was named Specter. The reason why Specter was banned was because 46 states adopted personally identifiable information laws, which developed safeguards for different data systems that held this information, which, in turn, rendered Specter useless[1].

Problems with data collection also come in the form of the action of collecting itself. The lack of cooperation in the cyber realm, between states and branches of government, are causes of great problems and concern. Informal talks that identify areas of international agreements, regarding cyber security, would be effective to target the areas of public infrastructure as well as the economic and legal impacts of cyber security. The only problem with this,

[1] "Edward Snowden: Leaks That Exposed US Spy Programme - BBC News." BBC News. January 17, 2014. Accessed October 27, 2015.

The Future of Cyber Intelligence

By: Joseph Espinoza
Old Dominion University Model United Nations Society

though, is that it is all hypothetical. The only problem with the summits and talks is that no one knows how to improve cyber security if the problems that it is meant to solve cannot be measured.

UN and International Responses

The first major work of action on crimes committed specifically via the internet came in Sept. 2001 with the Convention on Cybercrime held in Budapest. The convention and its corresponding treaty signified the first international treaty about internet crimes, and sought to bridge the gap between international domestic laws regarding behavior like copyright infringement, fraud, hate crimes, and issues regarding network security. Most of what this convention and treaty looked to do was act as a facilitating document for international cooperation when it comes to preventing, labeling, and punishing cyber-crimes. The treaty also includes that materials essential in the legal procedures such as evidence and the extradition of the accused are to be treated as any other crime. The treaty is signed by 47 countries total, and though it was created by and within the Council of Europe several countries have signed and ratified the treaty, including, but not limited to, Canada, Australia, the Dominican Republic, Mauritius, and Japan[2]. Later in 2001 and into 2002 the Council of Europe drafted an additional protocol to the Convention on Cybercrime specifically about the criminalization of xenophobic and racist actions via cyber systems. The protocol has 22 states party to it[3].

In 2012 UN Secretary General Ban Ki-Moon appointed a governmental panel of experts from 15 states called the "Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security" to create a report for the UN on the topic of developments in cyber-security and information technology, and to recommend international actions or

A Meeting of the appointed 2013 GGE
Source:
http://blogs.cfr.org/cyber/files/2015/04/8411021512_62b5b845e8_o-CD.jpg

[2] "Convention on Cybercrime." Council of Europe. September 23, 2001. http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm.

[3] "Additional Protocol to the Convention on Cybercrime." Council of Europe. January 28, 2003. http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm.

an opinion on it. The expert panel comprised of the 5 permanent members of the Security Council and ten other countries appointed from around the world, with Australia chairing. The report is now seen as a seminal work, and shaped the international understanding of cyber interactions and security. The report highlights four main areas to be addressed: cooperation, international law, confidence building measures, and improving state IT capacities. In the international law area of discussion a key consensus was reached among the 15 state exerts: international law fully applies to state actions in cyberspace. This means that state actions against other states, aggressive or not, or when states are in breach of any other international law, the same consequences should follow if the law/norm was broken in either cyberspace or ordinary space[4]. Here is a link to the landmark report, in total it is 13 pages long and is THE defining document for the UN thus far in the realm of cyber security. The UN's action on cyber security has for the most part been delegated to the General Assembly, specifically first committee (DISEC), and reactions to the 2013 report still top discussions on the committee agenda. In June of 2015 DISEC asked Ban Ki-Moon to appoint a fifth Governmental Group of Experts of 20 representatives. The report's four major findings include: the existence of state sovereignty in cyberspace, that international obligations made by states are applicable in cyberspace, states cannot use proxies to break international law and norms, and the recognition of the UN as the principal organization for the establishment of fundamental principles on the topic. The report will be presented to DISEC in October of 2015, and seeing as this Issue Brief will be published prior to this, here is a link to where the report will be published to, and where a list of UN resolutions and reports can be found[5].

Current Situations

Although this is not all the countries in the international community, the countries below have either committed cyberattacks on other countries, been caught hacking into other countries, or have initiated cyber security programs.

The United States of America:

The United States, not including their domestic cyber security programs, have an extensive and in-depth reach into other countries affairs. An example that occurred in July of 2015 was the investigation of the NSA's spying on Germany and whether or not the German intelligence agency knew it was occurring. Although this is not new for the NSA, it was revealed that the NSA was also intercepting German Chancellor Angela Merkel's cell phone communications. In addition to Angela Merkel, the NSA was spying on other ministers of Germany including the minister of finance which stated that Chancellor Angela Merkel

[4] Wolter, Detlev. "The UN Takes a Big Step Forward on Cybersecurity." Armscontrol.org. September 4, 2013.

[5] "UNODA - Developments in the Field of Information and Telecommunications in the Context of International Security." UN News Center. 2015.

By: Joseph Espinoza
Old Dominion University Model United Nations Society

"professed to be at a loss" during the decision to take action in the Greek financial crisis. This incident wouldn't have been made public if WikiLeaks, another form of a cyber security breach, was not allowed to have this information. WikiLeaks is an international journalistic organization that publishes secrets from other government's secrets, news leaks, and other forms of classified media online[6]. Other cyber security incidents that have occurred, even within the last year for the United States has been, the attacks led by Lizard Squad, who have taken credit for the Denial-of-service attacks on PlayStation networks, Xbox live, as well as an attack on North Korea and disruption of some gaming services on Christmas day of 2014[7].

China-

China has been hacking into countries in an increasing amount within the last two years. In May of 2013, China hacked the headquarters of the Australian Security Intelligence organization. In early 2011, the Canadian government claimed that Chinese hackers had compromised several departments of their federal government. In 2014, Chinese hackers also comprised computer systems within the Canadian National Research Council.

The United States and China have had many encounters of cyber-warfare, which has elevated the paranoia, and level of distrust of both countries. The feud between the Chinese and American government has reached the point of fever-pitch that the Chinese Embassy in the United States has stated that the accusations of cyber security against China are a direct result of sinophobic paranoia. The American government have the right to be paranoid due to the fact that, in October of 2014, the U.S. Federal Bureau of Investigation said that Chinese governments have been able to hack into computer systems of US airlines, technology companies, and other contractors involved in the movement of U.S. troops and military equipment.

In 2010, Google reported a targeted attack on its corporate infrastructure and was able to trace the attacks to China. These attacks resulted in the theft of intellectual property from Google. The Obama administration called this cyberattack, and many like it, an increasingly serious threat to US critical industries. Even though the United States has been a constant target of China from cyber security attacks, the only state that has not been attacked is North Dakota.

China has also been linked to the creation and use of Stuxnet. Stuxnet is widely believed to be a jointly built American and Israeli computer worm, although it has never been confirmed nor denied by either state. The use of Stuxnet was to sabotage the use of Iran's nuclear program during George W. Bush's presidency. The virus was so effective that in August of 2010, 60% of the computers worldwide that were infected were in Iran. The use of Stuxnet is to specifically target

[6] Tapper, Jake. "Obama Administration Spied on German Media, Government - CNNPolitics.com." CNN. July 4, 2015. Accessed October 27, 2015.
[7] Fung, Brian, and Andrea Peterson. "Meet the Grinch Who Stole Christmas for Gamers: The Lizard Squad." Washington Post. December 26, 2014. Accessed October 27, 2015.

By: Joseph Espinoza
Old Dominion University Model United Nations Society

the automation of electromechanical processes that are used to control machinery on factory assembly lines, amusement rides, or centrifuges for separating nuclear materials[8].

In a four-day discussion, both China and the United States had a "frank and open exchange about cyber issues." The use of cyberattacks against the United States are a red line for the Obama administration and regard these attacks as a core national security threat and will treat it as such. Despite four days of talks on comprise for the use of cyber security; China denies the accusations of cyberattacks on the U.S[9].

Russia-

During the summer of 2015, Russian hackers were able to shut down the Pentagon for over eleven days. This massive breach affected more than 4,000 military and civilian personnel and resulted in shutting down the Department of Defense for a few days. In addition to this hack on the Pentagon, it is speculated to believe that Russia has been able to steal as many as 10 million Americans' IDs along with current and former government employees. Russian hackers have been cited for using a cyberattack that relied on an automated system that rapidly gathered massive amounts of data and then sent the information gathered to thousands of Internet accounts within minutes. American sources state that the Russian attack was planned using encrypted social media accounts ranging from Snapchat to Twitter and Facebook.

Country Positions

Many countries submitted national plans and their positons on cyber security to the Secretary General in response to a section of UNGA resolution 69/28. These country responses can be found by following this link[10].

Canada:

Canada is one of the most active members of the international community in cyberspace. The country sat on the Group of Governmental Experts (GGE) and helped author its subsequent landmark 2013 report mentioned above. Canada is an avid supporter of the views of the report, especially in the areas of international law and the improvement of state IT capacities. Canada launched its own "cybersecurity and action plan of Canada" and new anti-spam legislature on the national level. Canada also routinely assists international organizations such as the Organization of American States (OAS), the North Atlantic Treaty Organization (NATO), and the Association of South East Asian Nations (ASEAN) both financially and with expert opinion in the field of cybersecurity[11].

[8] Zetter, Kim. "An Unprecedented Look at Stuxnet, the World's First Digital Weapon." Wired.com. November 3, 2014. Accessed October 27, 2015.
[9] "Chinese Hacked Government Computers, Ottawa Says." The Globe and Mail. July 29, 2014. Accessed October 27, 2015.
[10] "UNODA - Developments in the Field of Information and Telecommunications in the Context of International Security." UN News Center.
[11] Ibid.

By: Joseph Espinoza
Old Dominion University Model United Nations Society

The Republic of Korea:

In 2014 the Republic of Korea was the victim of attempted cyber-attacks against a power plant in the country, and since in cyber policy has been strengthened in the country. In March of 2015 South Korea created new cabinet positions for cyber security, and as one of the authors of the 2013 report, is a major supporter of its themes. The country began regional efforts to discuss cyber security by hosting the Asia-Pacific Regional Seminar on International Law and State Behavior in Cyberspace in 2014 jointly with the UN Institute for Disarmament Research, and the Seoul Conference on Cyberspace. South Korea still now heavily supports regional programs[12].

The Group of 7:

In mid-2015 the Group of 7 (G7) held a conference specifically regarding cyber security, and a new major focus of the group emerged: cyber security in the energy sector. The Group of 7 consists of Canada, France, the USA, Germany, Italy, Japan, and the U.K. with the European Union as a special member. The G7 was formally the G8, but the suspension of Russia from member ship has changed the group. The former G8 consists of over 50% of the world's GDP, incredible considering eight countries constitute the same economic output as 187 countries (including China). Non-coincidentally these states also constitute some of the most advanced cyber-states on Earth, and routinely discuss new issues of cyber intelligence and security.

NATO/Estonia:

In late 2007 into early 2008 treaty member Estonia was the victim of a cyber-attack. Civilians were denied service and government sites were spammed and forced to crash. Estonian officials quickly denounced Russia for the cyber-attack (the attack happened during a dispute between Russia and Estonia), but no evidence links Russia to this attack to date. Immediately following the attack on a NATO member, the alliance crafted its first cyber defense policy in January 2008. Later in 2008 the NATO Cooperative Cyber Defense Centre of Excellence (NATO CCD COE) was constructed in Tallinn, Estonia. This center now serves as the world's most advanced cyber defense facility, and is NATO's main cyber security organ. Each year the CCDCOE hosts a cyber security convention called "Cycon" to discuss developments in the field[13].

The African Union:

More often than not, African Union (AU) member states fall victim to the north/south technical divide. This means that often the less developed infrastructure and economic exploitation of the global south results in a technology divide leaving the global south in a less than advantageous

[12] Ibid.

[13] "Cyber Security." NATO. September 1, 2015. Accessed September 25, 2015.

By: Joseph Espinoza
Old Dominion University Model United Nations Society

position. The African Union has worked to bridge this divide, and beginning in 2009 the AU began to host conferences for its member states to draft legislation concerning cyber affairs, especially targeting issues relating to access and security of mainframes. The AU has worked closely with the UN Economic Commission for Africa (UNECA) concerning IT security and access. The 2009 Extra-Ordinary Conference of African Union Ministers in charge of Communication and Information Technologies was hosted in Johannesburg, South Africa and looked to unify cyber policy in the AU, which is still a goal of the organization to this day[14].

The Statue that sparked the Russia-Estonia Feud
Source:
http://news.bbc.co.uk/2/hi/technology/6290102.stm

[14] "Cyber Security." African Union. Accessed September 25, 2015.

Conclusion

When Snapchat and Twitter can bring down government agencies, and when some of the most powerful states attempt to fix problems that can't be measured, what will the international body be able to do to cease the relentless attacks of cyber warfare? Is the answer to make cyber terrorism a capital offense, or is the answer to ramp up the amount of cyber terrorism for the interests of national security? Some questions to consider are:

1) How does the role of access and accessibility play a role in cyber terrorism? Does this mean smaller countries with slower broadband are not allowed to join in cyber warfare?
2) Should the ICJ put groups like Lizard Squad on trial for their crimes?
3) How will the United Nations set an example for internet use?

Bibliography

"Additional Protocol to the Convention on Cybercrime." Council of Europe. January 28, 2003. Accessed September 24, 2015. http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm.

"Chinese Hacked Government Computers, Ottawa Says." The Globe and Mail. July 29, 2014. Accessed October 27, 2015.

"Convention on Cybercrime." Council of Europe. September 23, 2001. Accessed September 24, 2015. http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm.

"Cyber Security Primer." What Is Cyber Security? Accessed October 27, 2015.

"Cyber Security." African Union. Accessed September 25, 2015.

"Cyber Security." NATO. September 1, 2015. Accessed September 25, 2015.

"Edward Snowden: Leaks That Exposed US Spy Programme - BBC News." BBC News. January 17, 2014. Accessed October 27, 2015.

Fung, Brian, and Andrea Peterson. "Meet the Grinch Who Stole Christmas for Gamers: The Lizard Squad." Washington Post. December 26, 2014. Accessed October 27, 2015.

Tapper, Jake. "Obama Administration Spied on German Media, Government - CNNPolitics.com." CNN. July 4, 2015. Accessed October 27, 2015.

"Tech Talk to Help with China-US Discussions - CCTV News - CCTV.com English." CCTV News. September 24, 2015. Accessed October 27, 2015.

"UNODA - Developments in the Field of Information and Telecommunications in the Context of International Security." UN News Center. 2015. Accessed September 25, 2015.

Wolter, Detlev. "The UN Takes a Big Step Forward on Cybersecurity." Armscontrol.org. September 4, 2013. Accessed September 24, 2015.

https://www.armscontrol.org/act/2013_09/The-UN-Takes-a-Big-Step-Forward-on-Cybersecurity.

Zetter, Kim. "An Unprecedented Look at Stuxnet, the World's First Digital Weapon." Wired.com. November 3, 2014. Accessed October 27, 2015.