ODU United Nations Day 2016
Issue Brief

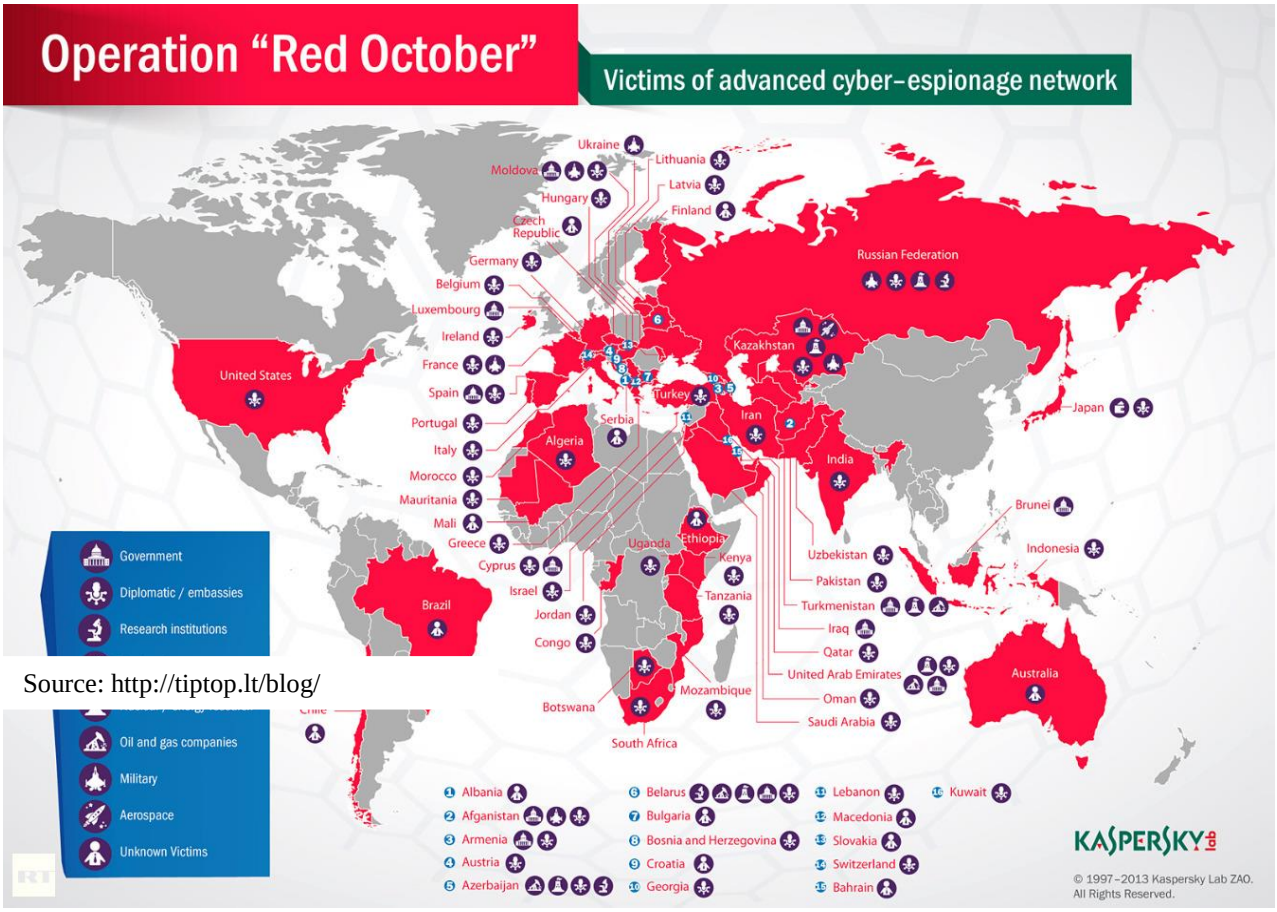
Combating Cyber Security Threats

by Joseph Espinoza and Kleopatra Moditsi
Old Dominion University Model United Nations Society

Introduction

Cyber intelligence gathering is, by far, one of the most effective means of collecting and storing large amounts of data, while at the same time risking crippling entire economies, exposing classified information, and even destroying entire nuclear weapon plans, all from the comfort of your own home. States recognize this imminent threat in a world growing more technologically connected than ever and develop distinct cyber security branches in order to defend their citizen's identities and confidential military tactics.

In a case of a cyber security violation, the flaming questions are "How did hackers do it?" and "What information did they get?" The purpose of this committee is not to concern itself with technical terms and practices of computer hacking. However, the consequences of such practices can keep many diplomats and country



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

leaders up for several days. Since cyber threats have emerged as a result of technological advancements and globalization, what can the international community do to prevent and/or eliminate these threats? 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. Two useful 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 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

One of the most well-known data collection scandal to occur in the past five years is the case of Edward Snowden and the United States National Security Agency (NSA). In May 2013, Edward Snowden, a former contractor of the NSA, revealed that his former employer was illegally collecting telephone records of millions of Americans and hundreds of millions of people globally. Further investigation revealed that NSA had been tapped directly into the servers of nine Internet firms, including Google, Microsoft, and Facebook.

Regardless of the morality of Snowden's

NSA Whistleblower Edward Snowden
Image Source: Al Jazeera

actions, the exposure of NSA practices to foreign audiences has created the image of a paranoid, unrestrained and vulnerable U.S. government.

Another recent example of cyber threat was the infamous Panama Papers of 2016. When an anonymous source contacted the German magazine *Süddeutsche Zeitung*, no one could imagine what would follow. Encrypted documents from Mossack Fonseca, a Panama-based law firm, showed the company selling anonymous offshore access to celebrities, politicians, athletes, and drug smugglers, to anyone trying to evade their own government. The trove revealed 11.5 million documents on hundreds of thousands of prominent clients. Banks that had partnered with Mossack Fonseca were humiliated and subject to prosecution. To mention all the states involved in the Panama papers would take endless pages, but a few are Kuwait, Libya, Qatar, Russia, Saudi Arabia, Turkey, and the U.S. Other companies undoubtedly have offered comparable services.

Problems with data collection and sharing come in the action of collecting itself. The lack of cooperation in the cyber realm causes great problems and concerns. States have to choose between cooperation in sharing counterintelligence techniques and maintaining the monopoly over those practices. Public infrastructure is another useful topic for discussion, since some countries are unable to secure sensitive information because they are less technologically advanced. The only problem with such summits and talks is that instead of tackling an already existing issue, the international community addresses problems in a preemptive manner, meaning before they arise and therefore before they can be measured.

UN and International Responses

The first major work of action on crimes committed specifically via the internet came in September 2001 with the *UN Convention on Cybercrime*, negotiated in Budapest. The treaty signified the first international treaty about to define and standardize responses to Internet crimes. It 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 aimed at was to act as a facilitating document for international cooperation when it comes to preventing, labeling, and punishing cyber-crimes.

A meeting in Geneva of the UN Group of Government Experts. Source: Council on Forgien Relations

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, though created by and within the Council of Europe, has been signed and ratified by several countries outside the Europe area, including but not limited to: Australia, Canada, Dominican Republic, Japan, and Mauritius[1]. Later in 2001 and into 2002, the Council of Europe drafted an additional protocol to the Convention on Cybercrime specifically

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

about the criminalization of xenophobic and racist actions via cyber systems.
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 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[2]. The landmark report is considered to 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 (GGE) to make recommendations. Their 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. A list of UN resolutions and reports can be found here[3].

Country and Bloc Positions

In the international community, there are states who initiate cyber attacks, states who are the victims of such attacks, and states who have been both the attacker and the victim in the past. Here's a brief list of major state blocks and important state positions on the matter:

African Union (AU): More often than not, AU member states fall victim to the north/south technical divide. Often the less developed infrastructure and economic exploitation of the global south leave the region in a disadvantage when compared to the technologically advanced north. The AU has worked to bridge this divide through conferences guiding member states in drafting legislation concerning cyber security. One such conference was the 2009 Extra-Ordinary Conference of African Union Ministries in charge of Communication and Information Technologies, which looked to unify cyber security policies throughout the AU, a goal yet to be achieved[4]. Another close partner of the AU on the matter has been the UN Economic Commission for Africa (UNECA) aiming at developing security mechanisms.

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

[2] Wolter, Detlev. "The UN Takes a Big Step Forward on Cybersecurity." Armscontrol.org. 4 September 2013.
[3] "UNODA - Developments in the Field of Information and Telecommunications in the Context of International Security." UN News Center. 2015.
[4] "Cyber Security." African Union, 25 September 2015.

its subsequent landmark 2013 report mentioned above. This state has been 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. Other actions include routine assistance to 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.

China: Chinese officials tend to view the Internet as an extension of national law and sovereignty, not an alternative. The key to the Chinese approach to internet security is the so-called 'Great Firewall', which enables the Chinese Communist Party to rigorously control the kinds of access possible within the country.

Chinese also agencies and organizations are thought to be heavily engaged in global Internet espionage in other countries. There is less evidence Chinese activists or officials try to use the Internet disruptively outside their country's borders, unlike Russia, where such actions are more normal. China usually support proposals for coordinated international action to better supervise the Internet.

Group of 7 (G7): The Group of 7 consists of Canada, the European Union (as a special member), France, Germany, Italy, Japan, the UK and the US. Non-coincidentally these states constitute some of the most advanced cyber-states on Earth and routinely discuss new issues of cyber intelligence and security. The main concern of Group of 7 (G7) revolves around cyber security in terms of financial institutions. Global cooperation is attempted in order to protect banks and investment firms, especially when these institutions are privately owned.

The Non-Aligned Movement (NAM): the 120 member of the UN"s largest voting bloc agree on the importance of cyber security, but insist that security preoccupations must not overshadow more fundamental issues of free and equal access o the internet. They are especially concerned that security concerns will be sued to strengthen the economic advances of wealthy northern countries, and justify the further impoverishment of disadvantaged peoples. Excessive cyber security they note, may contribute to global poverty, weaken already feeble governments, and worsen pressure for regional conflict and for international migration. Security, they note, must be combined with commitments to access and development.

North Atlantic Treaty Organization (NATO): In 2007, NATO member state Estonia was the victim of a Directed Denial of Service (DDoS) attack which shut down several networks temporarily. The attack happened during a nationalist dispute between Russia and Estonia, but no evidence links the government of Russia to this attack. Immediately after, the alliance crafted its first cyber defense policy in January 2008, and created the NATO Cooperative Cyber Defense Centre of Excellence (NATO CCD COE) in Tallinn, Estonia. Each year the CCDCOE hosts a cybersecurity convention to discuss developments in the field[5].

NATO stresses preparation for cyber defense. It does not engage in offensive operations, as a defensive alliance. This limits its ability to respond and undertake operations. NATO must wait to be attacked or for signs of immanent attack before it can respond.

Republic of (South) Korea: In 2014, the Republic of Korea was the victim of attempted cyber-attacks against a power plant in the country. Since, cyber policy has been strengthened in the country; South Korea created new cabinet positions for cyber security and is an author of the GGE report. The country began

[5] "Cyber Security." NATO. 1 September 2015.

regional efforts to discuss cyber security by hosting the Asia-Pacific Regional Seminar on International Law and State Behavior in Cyberspace jointly with the UN Institute for Disarmament Research, and the Seoul Conference on Cyberspace. South Korea still heavily supports regional programs.

Russia: Since 2007, hacking attacks from Russia have become a staple theme of media reporting. Foreign governments, especially NATO governments, and political parties are a common target, as critics of Russian foreign policy. The role of the government of Russia in this activity is unknown. The Russian government maintains that internet activity should be supervised to ensure its support national policies and goals.

In the meantime, China and Russia have signed a cyber security deal to mark cooperation between the two states. Its most significant features are a mutual assurance of non-aggression in cyberspace and support for cyber-sovereignty.[6]

United States of America: The US launched one of the first destructive cyber attacks, targeted against Iran's nuclear program in2 009, with temporary success. The United States also undertakes massive espionage against potentially all Internet and telephone users outside its borders, and some within.

At the same time, American officials want to strengthen global access to the Internet and minimize government supervision elsewhere. On the international level, the US aims at promoting internet freedom and shared practices for the creation of a secure and reliable cyberspace.[7]

Conclusion and Proposals

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?

Some alternatives for United Nations to consider include:

1) Can the UN Member States agree on Best Practices to guide Internet use and protection? What are standards and best prices that everyone in the UN can agree on?

2) Can UN Member states be asked to implement uniform standards for Internet security and supervision?

3) How to balance cyber security with individual rights? Do demands for cyber security require that private firms and users surrender much of their pervious freedoms to state government supervision and oversight? Some governments clearly favor such supervision, while others believe this is the opposite for what the Internet should do.

4) Should offensive attacks on the Internet—such as viruses that paralyze equipment, and Director Denial of Service (DDoS) attacks that jam networks, or attacks on specific operators—be prohibited under international law? If so, how should such a prohibition be enforced?

5) Finally, should there be a new UN agency to monitor Internet access and oversight? What should its powers be? How should it be financed?

[6] Yuxi Wei, "China-Russia Cybersecurity Cooperation: Working Towards Cyber-Sovereignty," Jackson School of International Studies, University of Washington, accessed Sep 19, 2016.

[7] Ibid.

Combating Cyber Security Threats

by Joseph Espinoza and Kleopatra Moditsi
Old Dominion University Model United Nations Society

Bibliography

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

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

"Cyber Security." African Union.

"Cyber Security." NATO. 1 September 2015.

"Cybersecurity." The White House. https://www.whitehouse.gov/issues/foreign-policy/cybersecurity

Obermaier, Frederik, Bastian Obermayer, Vanessa Wormer et.al. "About the Panama Papers." Süddeutsche Zeitung. http://panamapapers.sueddeutsche.de/articles/56febff0a1bb8d3c3495adf4/

Rubin, Gabriel T. "G-7 Nations Race to Bolster Security Against Cyberattacks in Finance." The Wall Street Journal. 19 May 2016. http://www.wsj.com/articles/g-7-nations-race-to-bolster-security-against-cyberattacks-in-finance-1463687620

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

Wei, Yuxi. "China-Russia Cybersecurity Cooperation: Working Towards Cyber-Security Sovereignty." Jackson School of International Studies, University of Washington. 21 June 2016.. https://jsis.washington.edu/news/china-russia-cybersecurity-cooperation-working-towards-cyber-sovereignty/

Wolter, Detlev. "The UN Takes a Big Step Forward on Cybersecurity." Armscontrol.org. 4 September 2013. https://www.armscontrol.org/act/2013_09/The-UN-Takes-a-Big-Step-Forward-on-Cybersecurity.