Forum: General Assembly

Issue: Issue #102: International Cyber-Security

Student Officer: Spencer Coy

Position: Co-Chairperson of the General Assembly

General Overview:

The Internet is a global phenomenon which provides many benefits, such as access to information and development of ideas or culture, as well as having a relatively low and non-competitive cost. However, the openness of the Internet leaves the door open to various cyber threats, which can cause many problems. Due to the global nature of the Internet, the governments of nations are responsible to safeguard the people against such threats. An example of how nations regulate the Internet comes from China, which restricts the websites its citizens can visit, to protect its citizens from potentially harmful information. The most major UN resolution to pass on this topic is an affirmation of the Internet as a human right in the Universal Declaration of Human Rights in 2016, which further reinforces the responsibility of all countries to protect its citizens against cyber-crimes; which can only be done together.

Importance:

The Internet provides many benefits to everyone, both social and economic. However, it also comes with a couple of drawbacks that affect all internet users, in every country. In the social realm, the Internet provides access to a variety of services previously unattainable by anybody, which is now able to be accessed by anybody. As well as being a nexus of knowledge the size of which was previously impossible. The Internet provides a unique set of tools and opportunity for the arts, human expression, and communication. Additionally, given the Internet's role in human progress and development, a 2014 survey by the Centre of International Governance Innovation (CIGI) revealed that 83% of the 23,376 respondents, chosen from 24 different countries, believe that the Internet should be a human right.

In economic terms, the Internet has many positive qualities. First, there is little to no competition for the use of the Internet, as it is practically a limitless resource and there is little cost to access it. Also, the Internet benefits from increased users, because as the amount of internet users increase, the individual cost decreases and the scale of the Internet increases. However, there are a several difficulties, such as cyber-piracy and illegal access of paid content on the internet. Also, the regulation and encouragement of ISPs (Internet Service Providers) is something countries require to do. Yet, the most pressing issue with the Internet is cyber-security. Issues pertaining to cyber-security, such as cyber-terrorism and cyber-crime, present potential disruptions in all the positive uses of the internet, as well as threaten global security. Issues such as the recent Russian involvement in the 2016 US elections highlight the strong need to combat such threats to international security. Thus, it is the responsibility of countries to regulate and counter such threats.

Examples:

China:

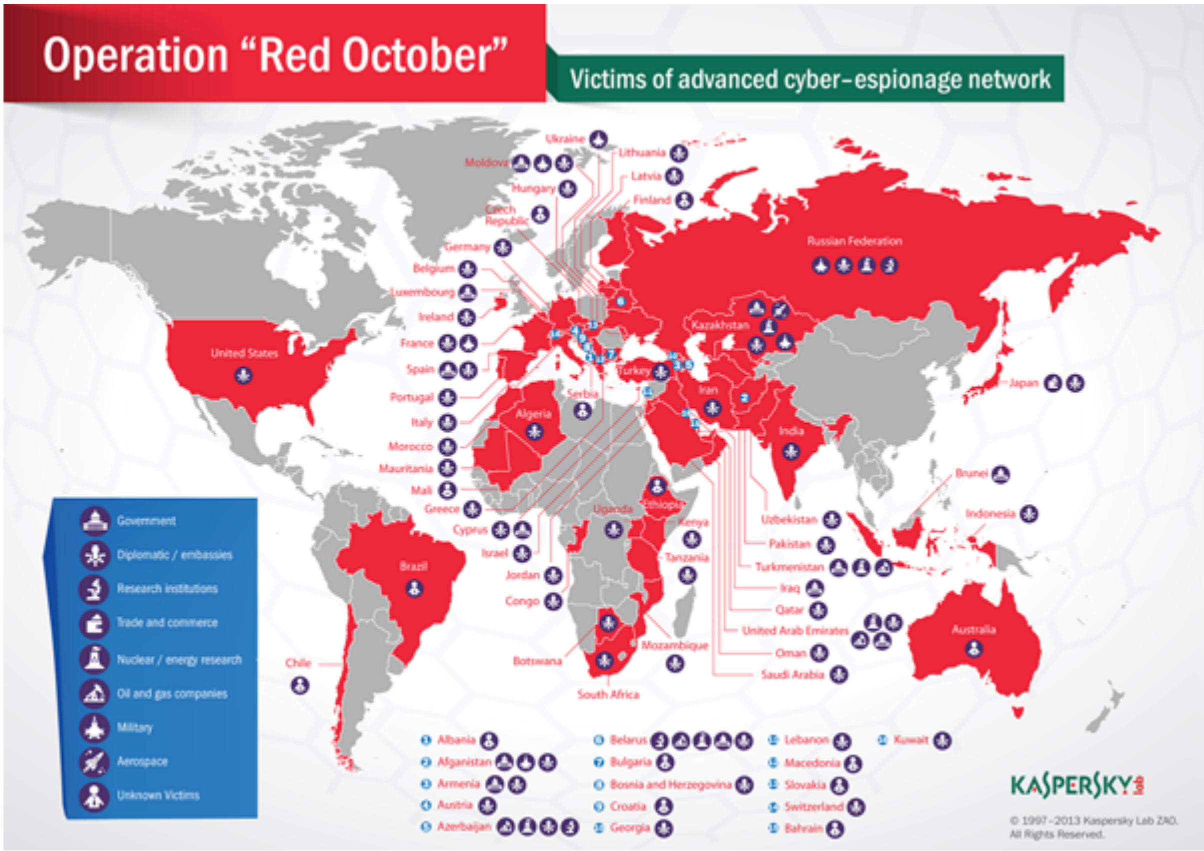
In China, the content that citizens can access is heavily regulated by the state. This is done by the Chinese government requiring Internet Service Providers (ISP) to block a predetermined list of URLs and keywords that have been deemed to contain potentially harmful information/content. Additionally, the government requires Internet Content Providers (ICP) to regulate the content they create. The government also has access to the emails and other personal information of its citizens and can access them if they are suspected of a crime. They heavily censor the internet to protect the public interest, and thus restrict the freedom of its citizens to access content for national security.

Spain:

Spain, on the other hand, regulates the use of the internet in a different way. The government allows for the free and open use of the internet for all its citizens and regulates the price and speed of the internet provided by their ISP (internet service provider). They conform to a governmental policy of net neutrality, which essentially means that all internet content and traffic is treated equally by ISPs, especially in terms of price, speed, and inclusion. Citizens have a right to open and fair internet access. In terms of cyber-security, they approach it in a different manner. They outline on their government website a set of principles and objectives that serve as a guideline on how to combat cyber-threats, which include goals to educate civilians and not to infringe on their privacy as much as possible. Lastly, Spain works with other countries to fight cyber-criminals as they cooperate with other countries in the European Union. The European Union (EU) is an economic cooperation between many countries in Europe. The EU provides a variety of benefits for member nations, such as the use of the Euro, freedom of movement and migration for citizens of member states, as well as other economic benefits. In terms of cyber-crime, in 2013 the EU adopted Cybersecurity Strategy, which provides a framework for support in case of a major cyber-attack, as well as informal channels for cooperation between member states' cyber-security agencies.

Red October Cyber-Attack:

The Red October or "Rocra" cyber-attack is a network of malicious computer software that infected a plethora of countries, discreetly gathering data from governments, embassies, research labs, and other important sectors. Originally found by Kaspersky Labs, an independent cyber-security firm, they found this international cyber-attack in 2012, which apparently had been operating since 2007. While this affected many countries, it affected Russia in particular. The most disturbing aspects to this cyber-attack is that the organization responsible is thought to be independent and that the cyber-attack happened without the knowledge of governments for five years. This computer virus covertly gathered intelligence for some unknown purpose, although it ahs been thought to have been sold on the black market.



https://securelist.com/the-red-october-campaign/57647/

History:

The most prominent official UN action in the realm of internet governance is an amendment to Article 19 of the Universal Declaration of Human Rights (UDHR) in 2016. This

Resolution also contains 15 recommendations on additional rights. These recommendations, unlike amendments to articles, are not binding nor enforceable. Additionally, expanding and regulating the internet is a part of many goals of the Sustainable Development Goals (SDGs), a set of goals to work on the betterment of people. It provides specific goals for governments over the next few decades, in which 193 UN members have signed, but the goals themselves are recommendations. Additionally, the General Assembly passed a resolution in 1999, which essentially promotes and request member states to inform the Secretary General of developments in information and telecommunications security. Next, Interpol, the UN international law enforcement agency has a cybercrime division, which assists member nations in advice and operations. They provide for multi-nation cooperation. The full 2016 resolution and 1999 can be found below.

2016 UN Resolution on the Internet

1999 UN Resolution

Key Terms:

- **Cyber-crime:** Crimes committed with the use of the internet. It differs from regular crime in that it is faster, more convenient, anonymous, and global without needing to share the physical location of its targets.
- **Cyber-terrorism:** The utilization of computer networks to disrupt national infrastructures or agencies and/or to intimidate a government or civilians.
- **Cyber-security:** The system of protecting networks, programs, and online systems from digital attempts to access, changing, or destroying information or otherwise disrupt/harm.

- **Internet Content Provider (ICP):** Organizations or website that put out services content on the internet, such as videos, files, news etc...
- **Internet Service Provider (ISP):** Companies that give access to individuals or organizations to the internet.
- **Net Neutrality:** The principle in which networks that provide internet service should not control the use of the network by its users or discriminate between content in terms of speed and accessibility.
- **Dark Web/Net:** The large area of the internet that is not accessed by conventual search engines, criminal use this portion to conduct illicit activities such as the sale of drugs/firearms, child pornography and more.

Questions to Consider:

1. What degree of independent sovereignty does each country have to regulate the internet, should they have any?
2. How much cooperation is necessary to effectively deal with international cyber-crime? What would this cooperation look like? How does your country feel about this?
3. What are the limitations that your country has in dealing with cyber-crime?
4. Consider the advantages and disadvantages of the internet, how does your country benefit from the internet? How much does your relay on it?
5. Given that the internet can be used for a variety of illicit activities (child pornography, arms dealing, organ/human trafficking) what is your countries stance on it?

Bibliography

II. How Censorship Works in China: A Brief Overview." Human Rights Watch, 2006, www.hrw.org/reports/2006/china0806/3.htm.

"Country Reports on Human Rights Practices for 2017-Spain." *U.S. Department of State*, U.S. Department of State, 2017, www.state.gov/j/drl/rls/hrrpt/humanrightsreport/index.htm.

"Cybercrime." N2018-092 / 2018 / News / News and Media / Internet / Home - INTERPOL, INTERPOL, www.interpol.int/Crime-areas/Cybercrime/Cybercrime.

"Cybersecurity." *España y El Magreb*, www.exteriores.gob.es/Portal/en/PoliticaExteriorCooperacion/GlobalizacionOportunidadesRiesgos/Paginas/Cibers.aspx.

Editors of Encyclopaedia Britannica. "Internet Service Provider." Encyclopaedia Britannica, www.britannica.com/technology/Internet-service-provider.

EP, Posted by Ask. "What Is the EU Doing to Combat Cybercrime?" European Parliamentary Research Service Blog, 7 Dec. 2017, epthinktank.eu/2017/11/30/what-is-the-eu-doing-to-combat-cybercrime/.

"Estrategia De Ciberseguridad Nacional." *Estadísticas Criminalidad En España 2016 | DSN*, www.dsn.gob.es/es/estrategias-publicaciones/estrategias/estrategia-ciberseguridad-nacional.

Gilroy, Angele A. The Net Neutrality Debate: Access to Broadband Networks. Congressional Research Service, 2018, The Net Neutrality Debate: Access to Broadband Networks, fas.org/sgp/crs/misc/R40616.pdf.

Howell, Catherine, and Darrell M. West. "The Internet as a Human Right." Brookings, Brookings, 4 Nov. 2016, www.brookings.edu/blog/techtank/2016/11/07/the-internet-as-a-human-right/.

"Infrastructure and Industrialization - United Nations Sustainable Development." United Nations, United Nations, www.un.org/sustainabledevelopment/infrastructure-industrialization/.

Mario, Rodrigo Canazza. "The Internet as a Global Public Good and the Role of Governments and Multilateral Organizations in Global Internet Governance." *Meridiano 47* 19 (2018)*ProQuest.* Web. 4 Aug. 2018.

"Resolution Adopted by the General Assembly-Developments in the Field of Information Adn Telecommunications in the Conte." *S/RES/1888(2009) - E*, United Nations, 4 Jan. 1999, undocs.org/A/RES/53/70.

"What Is Cybersecurity?" Cisco, 24 Aug. 2018, www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html.