The Threat of Cyber Terrorism and Its Outdated Investigative Process on a Global Scale

Daniel Weinert

Prof. Gaines

CYB-2500-001 / Spring 2018-2019

MSU Denver

The Threat of Cyber Terrorism and Its Outdated Investigative Process on a Global Scale

This paper will examine the threats of cyber terrorism that many nations are facing and how the cyber world has disrupted the global playing field. Since the rise of computer networks, we have seen the creation of techniques and tools to use the internet or other networks to either gain information, disrupt processes or plainly cause damage. This brings up great concern on how nations are allowed to use these networks and how they can investigate these types of acts against them. To find an answer to these just stated concerns we must first look at how the cyber world is treated by the international justice system.

To figure out the threats of the cyber world we have to first lay out what cyber attacks are and how they can be carried out. Firstly, we have to understand where this interaction happens. Most traditional types of attacks or crime occur on official theatres of war like lands, sea, air and space but cyber attacks are in the electronic space. Which is entirely manmade and not subject to any traditional laws or treaties. This electronic space is created, maintained and owned by public and private stakeholders. This creates issues on how to apply local and international laws and investigative jurisdiction (Melzer, 2011). According to the Tallinn manual the general term for cyber attacks is Computer Network Operations or CNO. This can be split into three types of activity:

1. Computer Network Attack (CNA) – Operations aiming to “disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.”

2. Computer Network Exploitation (CNE) – Operations aimed at collecting intelligence and data from adversary automated information systems or networks. This is linked to and has parallels with espionage.
3. Computer Network Defense (CND) – Actions taken to protect, monitor, analyze, detect, and respond to unauthorized activity within information systems and computer networks. And prevention of CNA and CNE through intelligence, counter intelligence, law enforcement, and military capabilities (Schmitt & Vihul, 2018).

Secondly, we need to look at how the justice system is set up on a global scale for these kinds of issues. At the moment most of the investigations and hearings are done on a local nation level. The International Court of Justice would be equipment with dealing with these kinds of issues, but the problem is that the international law is not set up to deal with these modern issues. Which makes this even a bigger problem is that even some nations don't have legislation concerning cyber-attacks. For example, Article 2(4) of the UN Charter prohibits the use or threat of force against the territorial integrity or political independence of a state, or in other words the legal restriction of going to war. The drafters of the UN Charter added a clause at the end, qualifying the prohibition to the threat or use of force to "or any other manner inconsistent with the purpose of the United Nations" (UN Charter, Art. 2). Now this part is kind of up for interpretations and many nations and experts are debating on whether cyberwarfare fits within this article. There are good arguments for and against it as for example the Vienna Convention on the Law of Treaties says that we should interpret such articles in good faith and it suggest with that, that we should adopt cyberwarfare under article 2. On the other hand during a UN Conference in San Francisco, Brazil wanted the threat of economic sanctions to be included to

article 2 and it got rejected which enforced the meaning that anything under article 2 has to result in direct destruction, injury, or death (The San Francisco Conference, 1945).

Let's look at some recent examples of cyber-attacks on nations. One of the most recent one happened in the Netherlands. Four Russian spies with computer hacking equipment were caught trying to gain access to the Wi-Fi network of the Organization for the Prohibition of Chemical Weapons. Luckily the Netherlands have a Defense Cyber Command which deals with these kinds of attacks. Since that the defense minister of the Netherlands has official said that the Netherlands are in a cyber war with Russia. He also said that the country offers its cyber soldiers services to NATO (Pieters, 2018). Another major story of cyber attacks was during the 2016 United States presidential election. We know the Russian government and independent Russian actors got access to up to twenty-one state's voting machines, the Democratic National Committee network and certain political figures email services (CNN, 2018). We also know now that there where concerns relating to Cybersecurity during the 2016 British Referendum vote on whether Britain should remain in the European Union or not. Members of the British Parliament have now come for suggesting that there is evidence that Russia might have had something to do with a DDOS attack that should down a voter registration page and might have hinder thousands of people from signing up to vote on this issue (Thompson, 2017).

Now let's see how these nations are handling these types of attacks. In the United States the Federal Bureau of Investigation has been the front running agency for massive scale cyber-attacks. During the United States 2016 election the FBI handled the DNC hack by launching an investigation and working together with the DNC's information technology department to figure

out the scale of the intrusion. After they finished their investigation, they forwarded their findings to the Justice Department which when in 2018 officially indicted twelve Russian spies operating under the Russian's intelligence agency GRU (CNN, 2018). In the situation that happened in the Netherlands, the four accused Russian agents were just deported immediately and not charged at that moment. The Netherlands are currently working together with the United States on a lawsuit against them (Pieters, 2018). Since 2017 the British Department of Defense has boosted training and funding to cyber defense programs as it seems to be to defenseless at the moment against these cyber-attacks (Allison, 2018).

To expand upon the investigative methods in the United States, lets take a closer looks at how the Federal Bureau of Investigations handles Cybercrime. According to their own website the FBI handles: "A cyber division at FBI headquarters to address cybercrime in a coordinated and cohesive manner, Specially trained cyber squads at FBI headquarters and in each of our 56 field offices, staffed with: agents and analysts who protect against investigate computer intrusions, theft of intellectual property and personal information, child pornography and exploitation, and online fraud" (FBI, 2016). As long as the cyber crime is being committed on and from U.S Soil the FBI is pretty successful in coming after these criminals but hence it is easy to commit cyber crimes from outside the country where the FBI loses restriction it can be very difficult to find and prosecute these criminals.

This brings us to the topic on how nations can seek justice against these types of attacks and how it is very easy for nation to launch these attacks as there no almost no repercussions depending on the nation in the scenario. If for example the origin nation of the attack does not

have any laws against launching cyberattacks and/or don't have extradition treaties than nations are powerless against these types of attacks. In the example that has Russia as the aggressor it is very hard to punish them because they don't have extradition treaties and they can't be held liable on a global level because international law and the International Court of Justice is unclear on how to handle cyber related cases and issues.

There are currently countless hearings and panels around the world debating these issues of cyber-attacks on a global level. The problem seems to be though that the only way we can truly investigate these types of acts is if the all work together since the cyber world doesn't care what country it is happening in. So, without working together, there will always be physical hiding spots for these aggressors. Now the problem currently is that for example Russia controls votes in the UN and other platforms and is natural against reforms on this issue, since there are using the current set of rules to their own personal gain.

The second biggest problem seems to be that a lot of the current technology used in governments is outtraded, a lot of talented people go into the private sector instead of the public, and most current politician seem to have very little knowledge about technology in general, especially in the United States. There have been many Senate hearings about Cyber Secuirty, and nothing can get done because the Senators don't even understand even principles of technology to even ask or propose something that is based upon fact and/or knowledge (Cillizza, 2018). This brings me to propose that we need more people that understand these issues to be included in these conversations to make sure that we are staying on the right track and doing stuff that would be recommend by IT and Cyber Secuirty officials.

With concern to any relatively new development, the global society seems to be grappling with how best to deal with cyberspace and its concerns. What the individual sees as a tool and innovation that allows them to view and share content with the world, a nation state sees it as a tool to control and attacks other nation states and people with different interests. The original principles around non-aggression and mutual respect of sovereignty are being challenged due to their outdated language and concepts. What this means for international law is that states now have the responsibility to shape what the future of cyberspace will look like.

References:

UN. The San Francisco Conference. (1945). Retrieved April 10, 2019, from https://www.un.org/en/sections/history-united-nations-charter/1945-san-francisco-conference/index.html

Allison, G. (2018, March 08). UK to 'step up' cyber defence capabilities. Retrieved April 17, 2019, from https://ukdefencejournal.org.uk/uk-step-cyber-defence-capabilities/

CNN. (2018, November 24). 2016 Presidential Campaign Hacking Fast Facts. Retrieved April 10, 2019, from https://www.cnn.com/2016/12/26/us/2016-presidential-campaign-hacking-fast-facts/index.html

Cillizza, C. (2018, April 11). How the Senate's tech illiteracy saved Mark Zuckerberg. Retrieved April 17, 2019, from https://www.cnn.com/2018/04/10/politics/mark-zuckerberg-senate-hearing-tech-illiteracy-analysis/index.html

FBI. (2016, May 03). Cyber Crime. Retrieved April 17, 2019, from https://www.fbi.gov/investigate/cyber

Pieters, J. (2018, October 15). Netherlands in "cyber war" with Russia, Defense Minister says. Retrieved April 10, 2019, from https://nltimes.nl/2018/10/15/netherlands-cyber-war-russia-defense-minister-says

Schmitt, M. N., & Vihul, L. (2018). Tallinn manual 2.0 on the international law applicable to cyber operations: Prepared by the International Groups of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence. Cambridge: Cambridge University Press.

Thompson, I. (2017, May 26). Did Russia Hack the Brexit Vote? Retrieved April 17, 2019, from https://www.vanityfair.com/news/2017/04/did-russia-hack-the-brexit-vote

UN Charter. (1945). Retrieved April 10, 2019, from https://www.un.org/en/sections/un-charter/un-charter-full-text/index.html

Vienna Convention on the Law of Treaties. (1969). Retrieved April 10, 2019, from http://legal.un.org/ilc/texts/instruments/english/conventions/1_1_1969.pdf

Melzer, N. (2011). Cyberwarfare and International Law (pp. 1-38, Publication). UNIDIR. Doi: http://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf