By: Justin Healey
April 30, 2022

International Law and Terrorism in Cyberspace

Summary of International Law

In short, international law refers to the set of rules, principles, and regulations regarding the affairs of sovereign nations or citizens of different nations with each other. There are two main subdivisions of international law: public international law, which deals solely with the affairs of sovereign nations amongst each other and their counterparts, and private international law, which deals with the affairs between private people and citizens. Public international law is mainly comprised of treaties between specific nations, ratified documents from the United Nations (UN), North Atlantic Treaty Organization (NATO) and European Union (EU), as well as documents produced by other internationally recognized alliances. The principles outlined in international law are based on humanitarian grounds, world economic stability, acts of war, as well as numerous other areas aimed at maintaining international peace and a relative balance of power.

Current Application of International Law in Cyberspace

Due to the complex structure of the internet, it is virtually impossible to regulate international cyberspace through one body. Thus, international law alone does not have complete authority over the rules and regulations of international cyber affairs. Internet service providers, web browser providers, website operators, governments, and individual organizations all have their own regulations dealing with domestic and international cyber affairs. However, the Tallinn Manual, published by Cambridge University Press in 2013, is the most influential and referenced document regarding international law in cyberspace. The authors of the Tallinn Manual, a group of well-respected scholars and legal practitioners led by American Michael N. Schmitt, comprised the manual with the goal of translating current international law into the cyber-space context. Chapter one, rule 1, section 1 of the Tallinn Manual explains, “States may exercise their jurisdiction vis-à-vis cybercrimes and other cyber activities pursuant to the bases of jurisdiction recognized in international law (Rule 2).”[2] Rule two, section two of the chapter further elaborates, “It must be cautioned that it is possible under certain circumstances for someone who does not wish to be tracked to spoof the geo-coordinates advertised by his or her computing device … Actual physical presence is required, and sufficient, for jurisdiction based on territoriality; spoofed presence does not suffice.”[2] These sections of the Tallinn Manual provide a beautiful solution to the issue of jurisdiction over cyberspace that crosses nations’ borders; in summary, the sections state that a nation (a state) may only pursue action, whether diplomatically or by force, against an agent in a foreign sovereign nation if they can provide indisputable evidence regarding the physical location of that agent within a nation’s borders. This not only solves the issue of jurisdiction regarding international cybercrimes, but it also addresses the use of proxies and virtual private networks (VPNs) to spoof one’s location. Due to this extraordinarily common and simple ability, the Tallinn Manual states, a nation must provide proof that the accused agent was physically within a foreign nation's borders before acting or assigning jurisdiction – a potentially spoofed IP address is not enough.

Recent International Cyberspace Incidents

Amid the current conflict between Russia and Ukraine, every major news outlet has covered at least one story from the many cyber-attacks during this war; for example, when Russia preceded their ground campaign into Ukraine with a series of cyber-attacks that shut down Ukrainian military and government websites. The Russians are also suspected of hacking a major satellite service provider, ViaSat, and disrupting internet services across Europe – this included shutting down Ukrainian military communications.[3] The media, although very thorough in covering these incidents, rarely shifted their spotlight to the countless other cyber-attacks that have happened this year (2022) alone – many of these incidents went uncovered for long periods of time. In March, white-hat hackers linked the Chinese government to an international cyber campaign that penetrated the networks of at least 6 U.S. states.[3] Also in March, malicious hackers targeted an Israeli telecommunication provider. The bad actors were able to shut down several Israeli government websites, and in the process delivering a painful blow to the Israeli economy.[3] In February of 2022, North Korea hackers were linked to a string cyber-attacks from 2020-2021, through which they managed to steal over $50 million from three different cryptocurrency exchanges. The U.N. claims that the North Korean government used the money to fund their nuclear weapons program amidst crippling sanctions imposed on the country.[3] Especially this year, it has become obvious that international cyber-attacks are not always about "who can do it better." The Russians used devastating cyber-warfare tactics as a preamble to their malevolent campaign into Ukraine, the Chinese have been using cyber-attacks and strategies to gain intelligence on their competitors on the world stage, particularly the United States, while at the same time North Korea allegedly stole more than $50 million to fund a nuclear arms program that the world is trying to prevent. Many of these malicious incursions went unnoticed for years; meaning, the governments/actors behind them never wanted credit and never tried to prove a point, but instead hoped their targets would never find out. This is a concerning thought as it raises some alarming questions – how many other attacks have there been that we don't even know about, and how much classified intelligence do foreign nations really have on us?

Dealing with International Cyber-attacks

Dealing with international cyber-attacks is often a seemingly impossible task. On one hand, the attacking country has malicious intentions and launched malicious attacks – if interpreted based solely on international law most of which would be acts of war, subsequentially leading to devastating global conflict. On the other hand, the targeted country risks retaliating unprovoked if they cannot prove with absolute certainty that the attack came from a foreign nation. In most cases, this is impossible. The incredibly easy ability to spoof one's location using a VPN or proxy makes for an incredibly challenging time in trying to trace the true origin of an attack. Moreover, even if an organization can prove the physical origin of an attack, it is almost impossible to prove who was behind the machine that the connection came from. If, for example, a bad actor was trying to start global conflict for personal motives or wanted to frame Russia for an attack, he/she could set a VPN to a server in Russia and then conduct a malicious cyber-attack on the United States. The IP address and the attack would appear to originate in Russia, but could have come from within the United States itself. This is where governments need to exercise extreme caution: before retaliating against a cyber-attack, they must be certain that the attack came from the accused country. Otherwise, they risk a potentially world-shattering unnecessary global conflict – especially if the two countries in question are the United States and Russia, the two nuclear superpowers of the world. The use of VPNs and/or proxies does not, however, always completely hide the real location of the attacker. In some cases, it is possible to pinpoint the real origin of the attack, but it often takes a lot of time and resources.

The incident at the 2018 Winter Olympic Games held in South Korea is an epitome of the necessity of a thorough investigation into any international cyber-attack. In the attack dubbed "Olympic Destroyer," Russian hackers were able to disrupt television and internet systems at the games with a single malware file.[6] They deliberately left false clues – false flags and signatures – designed to make the attack appear to have originated within many different countries. These false clues caused even the most experienced IT and cybersecurity professionals in the world to discount Russia as a potential culprit. A long three days after the attack, Cisco analysts downloaded the code from a popular database of malware samples and reverse engineered it. Within the code, they discovered key commonalities to previous cyber-attacks that the Russians had already been proven guilty of, including NotPetya and Bad Rabbit.[6] Through further analysis, cybersecurity analysts discovered hidden signatures within the code that were known to the North Koreans. In addition, there were countless other clues that seemed completely uncorrelated. Some pointed to the Chinese, some to North Korea. An analyst eventually discovered that the header of the malware file contained metadata which gave clues as to what programs were used to write the code. The header indicated programs that only the North Koreans were known to use, explicitly pointing to North Korea as the culprit. After many days and sleepless nights, a different analyst discovered that the header was forged. Then, a third analyst halfway across the world in Washington D.C., with vast experience with Russian cyberwarfare, was convinced the Russians were behind the attack. He based his assumption on code within a word document from Olympic Destroyer which was laced with malware that linked back to a 2017 Russian attack against Ukraine.[6] This analyst, Matonis, was later able to create a comprehensive web of the IP addresses and servers that the hackers had used to remotely control the attack at the games. Through incredible intuition and the help of his photographic memory, Matonis found a fingerprint that traced back to the largest Russian attempt to meddle in U.S. elections; in other words, Matonis proved with near certainty that the Russians were behind the attack on the Olympic games.[6] The U.S. government came to the same conclusion before Matonis, but there was no way to check their findings. In the end, Russia was proven culpable for the attack; however, it took months, thousands of analysts, dozens of agencies, and some of the brightest minds in the computer science industry to prove. Once again, it was imperative that the world possessed concrete evidence before retaliating to this international cyber-attack. If the incredibly sophisticated and deceiving clues left by the Russians were taken at face-value, North Korea would have been blamed for an attack they were not involved in, and the consequences could have been devastating to their economy.

As with any threat including cyber-attacks, the threatened parties would be within their rights to retaliate with force as outlined in international law; however, in doing so they create the risk of unnecessary conflict. As a result, many cyber-attacks, like Olympic Destroyer, occur without any major retaliation by the targeted party. MIT game theorists have considered this complication – they determined that there is a much higher chance that retaliation against a cyber-attack could backfire rather than bring justice to the culpable party.[4] Thus, the phrase usually used in context of nuclear holocaust, "mutually assured destruction," can be applied to cyber warfare. If every country retaliated against every cyber-attack, nations would be involved in constant international military conflicts, many of which could be unprovoked and lead to unnecessary losses for all parties involved.

Concerns of Cyber-terrorism

Along with the growing concern of cyber-warfare between powerful nations, the threat of cyber-terrorism has been rapidly increasing as well. Many civilians around the world are focused on the threat of physical terrorism, for example, the 2001 9/11 attacks or 2013 Boston Marathon bombing, and consequently are failing to see how cyber-terrorism can be just as devastating as the forms of terrorism the world is grievously used to. Every day, as we continue to thwart the many terrorist attacks against the United States and other targeted countries, these radicals are constantly looking for new ways to undermine our efforts. Even if terrorist organizations do not possess the capabilities to carry out a cyber-attack against a powerful government or nation, hacking groups around the world have demonstrated their abilities on countless occasions, and cash is king. Terrorist organizations could pay a rouge black-hat hacker or group to do their dirty work just as easily as they could pay an arms dealer for more weapons. As the use of computers, networks, and the cloud become more common, terrorists are going to find ways to exploit these technologies if they are not well guarded.

For example, the fast-moving electric car industry has brought concern to some security experts. Electric cars rely on computers to function; if a machine relies on computers, it is susceptible to being hacked. In January of this year, German 19-year-old David Colombo claimed he was able to hack into at least 25 different Tesla vehicles in 13 different countries.[5] He later clarified that he was not able to control the breaking, acceleration, or steering mechanisms in the car, but was able to lock/unlock doors, flash headlights, control the radio, and even start/stop the engine. Although David is a well-known and respected cybersecurity expert and he does not possess any malicious motives, he proved that it is possible to hack into electric cars with the current security measures in place. Although he was not able to gain control of the steering, breaking, acceleration or any other means of interfering with the owner's driving, this does not mean that the possibility is not still there or that it will not be a concern in the future if we fail to recognize these threats now. If David was able to hack into the electric vehicles, what is stopping a terrorist from doing the same thing? David stated in his blog that he did not believe that he could have controlled the movement of the vehicles at all, but, if in the future a terrorist gained remote control of the steering/acceleration of a vehicle, they would possess the ability to use the vehicle, with the driver still inside, as a lethal weapon. Based on historical events, it is a fair assumption that some terrorist organizations would have no moral issue taking this a step further and weaponizing hundreds of cars in a city or country at a time and using them to wreak havoc and destruction to vulnerable citizens. It sounds like science fiction, but this form of terrorism is not that far from reality.

Besides weaponizing cars, cyber terrorists could also use unguarded networks to shut down entire electrical grids, as the Russian military already demonstrated is possible in Ukraine, as well as shutting down dams, targeting nuclear power facilities, or hacking into planes and other forms of public transportation. For such reasons it is imperative that cybersecurity experts around the world keep up with this constantly expanding threat in this constantly expanding field. With the proper security measures, it is possible to minimize or ideally prevent cyber-terrorism, but that goal is only possible if we remain vigilant and cautious to new threats. In 2002, we were worried about terrorists threatening pilots with ceramic knives on planes – today we need to be worried about terrorists controlling planes without even being aboard.

By: Justin Healey
April 30, 2022

Sources

1. *Carnegie Endowment for International Peace*. https://carnegieendowment.org/2021/06/14/brief-primer-on-international-law-and-cyberspace-pub-84763

2. Schmitt, N. Michael; The Tallinn Manual. http://csef.ru/media/articles/3990/3990.pdf

3. Center for Strategic & International Studies, "Significant Cyber Incidents." https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

4. *Help Net Security*, "Countries that retaliate too much against cyberattacks make things worse for themselves/." https://www.helpnetsecurity.com/2020/12/15/retaliate-cyberattacks/

5. Zilber, Ariel; *The NY Post*, "19-year-old claims he hacked into over 25 Teslas in 13 countries." https://nypost.com/2022/01/12/teen-claims-he-hacked-into-over-25-teslas-in-13-countries/

6. *Wired.com*, "The Untold Story of the 2018 Olympics Cyberattack, the Most Deceptive Hack in History" - https://www.wired.com/story/untold-story-2018-olympics-destroyer-cyberattack/