The Viability Of An International Treaty On Cyber Warfare

As cyberspace has grown over the years, it has ingrained itself in nearly every facet of our lives making it a necessity to get anything done. This rapid expansion has left a lot to be desired in terms of security and government legislation. Such dependence on devices and the information they provide us has given birth to a lucrative black market as well as a new medium for governments to spy and disrupt other countries. To safeguard themselves, large nations like Russia, China, and the United States have established cyber operations for both defensive and offensive purposes (Strohm, 2018). Coupled with numerous alleged state-sponsored attacks, many have begun to question what is being done around cyber in order to avoid any future catastrophic events. Due to its nature, however, managing a medium so vast without any borders has proven difficult. Not only is current legislation lacking behind new technologies, but it will continue to do so which means that governing the bleeding edge of technology is next to impossible. This has led to the discussion about the viability of an international treaty on cyberwarfare.

Among the arguments for such a treaty are that cyber warfare is still very much in its infancy meaning that countries are overly comfortable testing the waters for what may be acceptable. In a span of fewer than seven years, the world saw its most devasting cyber-attacks which included Stuxnet, WannaCry, and NotPetya that cost upwards of a billion dollars in damages (Sharkov, 2018). What is worse is that it was government entities that were in some way responsible for the attacks. This includes either allegedly being the conspirator behind it like Russia or the United States, or having an exploit leaked that made the attack more potent such as what happened with the NSA and WannaCry (Meyer, 2018; Anderson, 2012; Chappell, 2017). Despite many well-grounded accusations in these cases, there were never any real consequences. This clear failure to hold someone accountable does not do much in the way of discouraging this type of behavior in the future. By establishing an international treaty to help combat similar incidents, it would help make things clearer. Part of this solution would likely include implementing cyber rules of engagement. Not only would this help to provide a baseline for what is acceptable behavior, but it would hopefully provide consistent guidelines on the proper responses to given situations. Another possible outcome of such a treaty would be a collaborative force that shares resources and intelligence in order to protect mainly civilian and possibly military infrastructure. Since the barrier of entry for cyber operations is much lower in comparison to the cost of the military, it is much easier for smaller states and private individuals to carry out malicious attacks. By having a shared responsibility, it would be easier to deal with smaller threats that may include cybercrime and terror threats. However, the logistics would be very complicated, especially since many countries would likely be unwilling to share their most effective tools as well as differences in local laws. By providing a standard for countries to follow with better accountability and resource sharing, a treaty would certainly seem to make sense, but its overall effectiveness is still rather questionable.

Due to the ever-changing nature of the internet, establishing a meaningful set of concrete rules that can be agreed upon by the most influential countries in the cyber realm would be next to impossible. In all likelihood, even if something of value was ratified, it probably would not last for long due to how fast technology advances. In order to prosecute a State for wrongdoing, their actions would have to have been already defined as a violation and the magnitude of their crime

would have to be worth any blowback that might result from prosecuting them. This also begs the question of what attacks warrant a response? Given the range of what is possible in cyberspace, what falls under espionage, sabotage, or propaganda? Just defining what is not acceptable has the possibility of infringing on a State's sovereignty which raises its own set of issues. There is also the problem of who oversees prosecuting wrongdoing. Since the United Nations gives members in the Security Council veto power to block certain actions including the maintenance of treaties, having a meaningful treaty to prevent unfavorable cyber actions is unlikely (Wood, 2015). This is compounded by the fact that the council includes members such as Russia, the U.S., and China which are arguably some of the biggest players in the cyber arena today. The final and possibly weakest part of any is attributing the blame. Even in the most devasting attacks such as Stuxnet and NotPetya that happened years ago, there is still a small degree of uncertainty of the parties behind them. If we expect fair judgments across the board in relation to these types of incidents, we need to be able to reliable point the finger with enough evidence to back it up which is extremely difficult in this field. Such a treaty is more of a wish list that would have a difficult time delivering on what most would consider the bare minimum.

While I believe that clear rules are important to governing, I am extremely doubtful that such as treaty could be accepted by the more prominent States. With cyber law still in its infancy, there is still plenty of room left to iron out complex subjects. In addition, it is quite unlikely that countries will want to sign away their best cyber weapons. Smaller countries benefit greatly from being able to use this class of tools in comparison to spending hundreds of millions on military weapons. A better question than 'should we develop an international treaty on cyber warfare' would be 'how effective would it actually be?' Across the globe, countries are stockpiling their zero-day vulnerabilities, holes in hardware or software that the vendor does not know about (Zetter, 2014). Slowly, but surely, we are getting to the point where we were during the Cold War where nations were stockpiling nuclear weapons in the event that they were to be attacked. If we continue down this path, we likely won't need any sort of treaty as the threat of mutually assured destruction could be enough to intimidate others against the threat of cyberwar. Realistically, we are unlikely to see a treaty with proper regulations that are enforced fairly until we see an event that causes enough damage to warrant it. Regardless of what happens, it would be in the interest of all parties to take preventative measures that protect their domestic infrastructure instead of relying on a weak international agreement that can be broken.

With all things considered, should there be a treaty? Maybe, but it would likely be ineffective, and it would only be selectively enforced anyway. They are still several problems that stand in the way. For one, politicians are extremely underinformed on the topic of cyber security. This is demonstrated all the time whether in the recent US Senate hearings regarding Facebook and Google or Australian politicians calling for a 'side gate' to review suspicious activities (Borys, Doran, & Belot, 2018). Another problem is that cyber knowns no borders. This ties into the fact that lone actors can still attack practically every computer on the internet, and nothing can stop them except preventative measures such as bug bounty programs enacted by companies or legislation requiring that certain security measures be taken. Even if every country agreed to a given rule set, there are still rogue actors and terrorists with similar capabilities that do not sign these treaties. Cyber operations like Stuxnet have been proven to be rare and will likely remain that way, especially now that more countries have developed their own capabilities. If the main goal of a cyberwarfare treaty is to protect vital civilian and military infrastructure, there are better ways to accomplish it.