Conflict Resolution in Cyber World

Bhavneet Soni

Conflict Resolution in Cyber World

Cyber conflict can be of many kinds varying from social media trolling, to cyber bullying to international cyber ops. When dealing with online interaction or our cyber escapades there are some inherently troublesome barriers to our communication.

1. Projections and Transference – most of the nonverbal context is lost when communicating online, which leads to miscommunication and in some ways to conflict. We see the world through our desires, needs, goals, dreams, and emotions, and we anticipate those from other individuals. We tend to extend our projections what and how other should behave when we are online decisively in light of the fact that we don't have the visual or sound-related signs to guide us in our elucidations. How we hear an email or post is the means by which we hear it in our own particular heads, which could conceivably mirror the tone or state of mind of the sender (Munro, 2002).
2. Disinhibition Effect – It's well understood that individuals say and do things on the internet that they wouldn't usually say or do in person. Even though people are not total anonymous they feel more uninhibited and communicate without much thinking. This is widely called as "disinhibition effect" (Suler, 2004). Add to that if a person believes they are anonymous and can get away with it they can even indulge in criminal behavior.

There are personal conflicts, conflicts based on religions, politics and between nation states, for the purpose of this paper we will be keeping our focus on international dimension of this problem and will be discussing the international conflict between states. By the end of the twentieth century, even though it had been a few years since the creation of World Wide Web in 1991, it was evident that next generation of wars will most likely be caused by and fought in the cyber world. Cyber conflicts are just an extension of conventional conflicts and on this new battlefield, anyone

with access to internet – regardless of their physical location – can join the fight. We have seen this in a number of protests and demonstrations specialty in the Middle East during Arab Spring, unsuccessful military coup attempt in Egypt where public opinions and information dissemination via cyber world changed the outcomes. In 2016 US presidential elections cyber-attacks and hacking undoubtedly changed the face of the election. It has a very high probability to even take countries to war, in 2014 a Chinese national was indicted for hacking into computer networks of Boeing and other contractors. The perpetrator was a part of larger scheme to steam plans for F-22 and F-35 fighter jets and also for C-17 transport aircraft. It was not certain whom the people in China who authorized and funded this attack, however One report by a cybersecurity firm said hackers linked to the Chinese government kept up efforts to break into US computer networks shortly after the cybersecurity agreement (phys.org, 2016). These are only possible because the people perpetrating these attacks think and in some cases get away from being caught for the crime. USA has also indulged in such activities, as President Trump said on Feb 5, 2017 “Do you think US is so innocent”. The notoriously infamous malicious computer worm “Stuxnet” was churned out from the bowels of NSA and CIA with the help of Israel’s counterpart agencies. The worm was designed specifically to target Iran’s nuclear facilities. Stuxnet used zero day attacks on the PLCs controlling Uranium enrichment centrifuges only (Stuxnet - Wikipedia, 2014). The anonymity or perception of there off may lead to a situation of sabotage, one country can declare a war or another on perception that they have been cyber attacked by the latter. Like any other medium of communication States have been constantly using cyber space to push their agenda and propaganda on to the susceptible public. To have a grasp of how the cyber space has provided with different targets to be exploited and leads to increasing conflicts, in 2010 US Canadian researchers tracked a sophisticated cyberespionage network, Shadow network (Foundation, 2010). The network

specifically targeted Indian Ministry of Defense, the U.N., and the Office of the Dalai Lama (Kshetri, Cloud Computing in Developing Economies, 2010). Computer systems in these offices were affected with installation of malicious software. It targeted microphones, cameras, controlled keyboards, and downloaded emails (Simmons, 2011). According to Wikileaks documents thee attacks were directly linked to the Chinese government which could have led to a military global conflict. Societies today are confronted with a paradox, weather to disconnect from the internet or embrace it and be susceptible to all it brings.

For this reason, Cyber security is a worldwide issue that requires a universal arrangement. Conflict resolution in Cyber World requires be at both strategic and tactical level. To counter the increased dependence and increasing complexities of the modern computer networks better defense against an attack in a key sense can only be achieved by putting resources into future technologies and modernizing infrastructure (Kosovo, Cyber Security, and Conflict Resolution, 2014).

After the realization of the affects a cyber-attack can have on the economy and a countries security many states have started investing heavily in developing cyber offense and defense capabilities, and have seen them grow rapidly over the past years. However these advances have created various issues of their own. We need to have proper policies and practices in place. As seen in the NSA massive data collection exposed by Snowden how if unchecked these cyber capabilities can encroach upon citizens' rights. Also the hubris than the country with technological advantage can get away with anything, as we seen NSA spying on friendly countries and heads of states. Recent disclosures have highly impacted the moral standing of the country in the world.

Hence putting in place checks and balances for cyberspace activities of the state is very important and of increasing significance. It requires a development and installation of

comprehensive framework of rules and regulations (Kshetri, Cybersecurity and International Relations: The U.S Engagement with China and Russia., 2014). To do so we need to look into what are the challenges we face when coming up with these regulations and how we can address these. There are a number of unique points that gives us insight on the effects of these policies on national and international relations conflicts.

1. There are no stated or widely abided by set of international rules when it comes to cyber security. For example, while a host of unspoken norms guided the U.S.-Soviet Union relations during cold war era (Lipson, 1991), due to the recent development of these threats, there is not have not yet developed to guide international relations on the cyberspace due to its newness.
2. Another challenge is the nation states involved in cyber-attacks are generally inferred and circumstantial rather than straight forward. Its almost impossible to trace the origin of the software, which makes it difficult to confront and bring the perpetrator to the tasks.
3. The anonymity of the internet makes the perpetrations of such attacks easy and frequent as opposed to physical altercations which are rare and few.

To address these challenges there is a need to have more international cooperation and trust building measures. A countries jurisdiction end once the internet cable crosses out of its border. There is a need to put in place an international agency that would have jurisdiction and authority to implement and reprimand the culprits. Achieving such a big and power full organization will be quite difficult to come up with as there is huge disparity in technological advancement of various nation states. It’s more likely that regional political and military alliances will come up quicker and more tangible progress on strategic cyber security.

References

(2016, March 23). Retrieved from phys.org: https://phys.org/news/2016-03-chinese-national-hacking-defense-firms.html

Foundation, I. W. (2010). *Shadows in the Cloud: Investigating.*

Kosovo, Cyber Security, and Conflict Resolution. (2014, November 25). *2501 Research - Analysis - Editing - Publication*.

Kshetri, N. (2010). *Cloud Computing in Developing Economies.*

Kshetri, N. (2013). *Cyber-attacks and Cyber-warfare: Western and Chinese Allegations and Counter-allegations.*

Kshetri, N. (2014). Cybersecurity and International Relations: The U.S Engagement with China and Russia. *FLACSO-ISA.* Buenos Aires.

Lipson, C. (1991). Why are some international agreements informal? *International Organization*, 495-538.

Munro, K. (2002). Conflict in Cyberspace: How to Resolve Conflict Online. In J. Suler's, *The Psychology of Cyberspace.*

Simmons, B. A. (2011). International Studies in the Global Information Age. *International Studies Quarterly*, 589 - 599.

Stuxnet - Wikipedia. (2014). Retrieved from https://en.wikipedia.org/wiki/Stuxnet

Suler, J. (2004). The Online Disinhibition Effect. *CyberPsychology and Behavior*, 321-326.