David Schurman

Professor John E. Savage

Cybersecurity and International Relations

8 March 2017

Prompt 4

The Cyber Cold War

Ever since the end of the Cold War in 1991, relations between the United States and Russia have been stable. Now, however, tensions seem to be on the rise, because cyberspace has given the two nations a new arena to battle. The difficulty of attributing, or identifying, the source of cyberattacks allows the United States and Russia to covertly hack each other while avoiding physical confrontation. A recent, poignant example of this hacking was Russia's alleged cyber-espionage designed to disrupt the 2016 United States electoral process. The immense scale of the Russian meddling has made some liken it to an outright declaration of war. Already, the United States and Russia are competitively developing cyber-technologies and conducting cyber-espionage against each other, tactics much like the arms race and spying of the Cold War. Thus, Russia's interference in the United States election forecasts not only increased tensions between the two nations, but the beginnings of a Cold War fought in cyberspace.

The difficulty of attributing cyber activity allows nations to easily and covertly attack one another, even during peacetime, making cyberspace conducive to nation-scale conflict. Attribution stands as one of the most challenging cybersecurity issues to date, as it "requires a significant amount of time to complete" and often yields questionable or incomplete results (Hanson). The ability for attackers to remain anonymous incentivizes them to continue their cyber exploits, as an uncertain victim is less likely to retaliate. The U.S. Director of National

Intelligence stresses the severity of the attribution problem, citing it as a chief reason that "numerous actors remain undeterred from conducting…cyber espionage or perpetrating cyber attacks" (Hanson). Included among these actors are government agencies, which use malware to steal information and disable physical infrastructure. Cyberattacks have even become the go-to method for some countries to express displeasure with others, as they are "more forceful than a diplomatic statement but…short of lobbing a cruise missile into a foreign capital" (Hanson). As a result, many nations, notably the United States and Russia, "now have military and intelligence cyberwarfare units" primarily devoted to developing new pieces of malware and to reinforcing their own cyber defenses (Hanson). This bolstering of digital weaponry combined with systemic lack of deterrence has culminated in a cyberspace that is prone to conflict. Russia's recent involvement in the United States election provides an important example of such conflict.

Russia's meddling in the 2016 presidential election demonstrates that peacetime cyberattacks are a viable method for one country to exert influence over another while avoiding significant backlash. Throughout the 2016 United States election cycle, there were reports of a Russian "campaign of hacking, email leaks, and fake news" designed to "undermine public faith in the US democratic process, denigrate Secretary Clinton and harm her electability and potential presidency" (Pagliery, Dearden). By utilizing cyberwarfare techniques such as espionage and leaking of information, Russia had a profound impact on a major American event without ever using physical force. Additionally, by covering its tracks to make attribution more difficult, Russia managed to avoid any significant retaliation to their hacking. Although the CIA does possess enough evidence to conclude Russia's involvement in the election, the United States' lack of retaliation shows the effectiveness of attributional uncertainty at mitigating repercussions against an attacker (Pagliery). Without the fear of severe repercussions, Russia will not be deterred from committing future, potentially more damaging incursions. As Russia continues their digital aggression against the United States, relations between the two countries will continue to unravel. Experts have now begun to realize the very real potential for a full-fledged cyberwar between the United States and Russia.

The election meddling foreshadows an “arms race” of cyberwarfare technology and increased cyber conflict between the United States and Russia: a Cyber Cold War. Like the original Cold War, the so-called “war of bits and bytes” will be fought largely without large-scale physical violence, as cyberspace gives the United States and Russia an effective method of attacking one another while avoiding direct confrontation (Pagliery). A “cyber arms race” will develop and increase in momentum as the two nations competitively develop technology to “continue to test their adversaries’ technical capabilities, political resolve, and thresholds” (Hanson). As a demonstration of the severity of the situation between the United States and Russia, a NATO (North Atlantic Treaty Organization) commander likened the recent election meddling to an outright declaration of war, saying that this “blatant aggression…in a domain other than conventional warfare” could be worthy of provoking a NATO retaliation (Dearden). However, as cyberwar is such a novel concept, there exist few international policies defining what such a retaliation should even entail. Russia exploited this procedural uncertainty, as it did with attributional uncertainty, to attack the United States in a way that would not trigger a significant counterstrike. As long as the United States and international organizations do not clarify what constitutes an appropriate response to such attacks, aggressive nations will remain undeterred, and acts of cyberwar will continue to escalate (Hanson). The longer this escalation is allowed to continue, the more imminent the threat of a Cyber Cold War.

Both the difficulty in attributing Russia’s meddling in the 2016 United States election and the lack of protocols governing cyber conflict have made cyberspace ripe for a Cold War. As peacetime cyberattacks continue to occur, nations will continually bolster their technological offense and defense capabilities, resulting in a “cyber arms race.” Russia’s election meddling, one such attack, foreshadows the United States and Russia’s entry into their own cyber arms race and the possibility of a Cold War fought entirely in cyberspace. Until the United States and NATO better define norms and procedures for responding to cyberattacks, online war will continue unchecked. Going forward, international organizations should analyze patterns of cyberattack, determine a measure for severity of any given attack, and draft procedures for retaliation or punishment. It is of paramount importance that nations are prevented from waging cyberwar, lest we enter the era of the Cyber Cold War.

Works Cited

Dearden, Lizzie. "Russia's Meddling in US Election Could Be 'Act of Aggression', Says Nato Commander." *The Independent*. Independent Digital News and Media, 03 Mar. 2017. Web. 06 Mar. 2017. <http://www.independent.co.uk/news/world/europe/russia-donald-trump-hacking-us-election-act-of-war-collective-defence-nato-commander-donald-trump-uk-a7609551.html>.

Hanson, Fergus. "Norms of Cyberwar in Peacetime." *Brookings*. Brookings, 17 Nov. 2015. Web. 06 Mar. 2017. <https://www.brookings.edu/blog/markaz/2015/11/17/norms-of-cyberwar-in-peacetime/>.

Pagliery, Jose. "The Emergence of the 'Cyber Cold War'." *CNNMoney*. Cable News Network, 19 Jan. 2017. Web. 06 Mar. 2017. <http://money.cnn.com/2017/01/19/technology/cyber-cold-war/>.