B01085721

Professor John E. Savage

CSCI 1800

15 February 2017

The New National Cyber-Morality

The advent of cyberspace and the Internet has undeniably made the human race more interconnected than ever before. This increase in interconnectivity has had countless benefits—easier access to information, sharing of services, and and improved overall efficiency of industry, to name a few—but it is also not without its downsides. Namely, cyberspace is an almost completely free and unregulated platform in which users rarely face punishment for any immoral actions. As people traverse the world of cyberspace, hiding behind usernames, avatars, and the screens of their devices, their online behavior becomes markedly different than their normal behavior. The persistence of colloquially-named "Internet trolls," or online users who strive to insult and demean other users, shows that when someone is protected by a "no rules" environment their actions may become darker and more violent. This same principle applies not only to individuals, but also to larger entities such as nation-states, who use the free terrain of cyberspace to conduct espionage and attacks even in times of peace. The freedom and un-regulation of cyberspace allows nation-states to wage cyberwar with impunity, resulting in an aggressive and caustic "cyber-morality" that bears little resemblance to the morality of everyday life.

The unregulated nature of cyberspace allows for unprecedented online freedom, which has inspired users to do whatever they want with little regard for consequences. In fact, since its conception, the Internet was "was built on trust" and designed to be as open and free as possible

(Scola). Ever since the creation of the Internet, a hallmark of cyberspace has been this culture of ultimate freedom. Cyberspace allows anyone to accomplish anything that they want; according to the security company McAfee, "'the internet allows anyone to send anything anywhere and it will likely get there'" (Grauman 10). Such freedom has had undeniable benefits, such as increased ease of access to important information and efficiency of communication and connectivity, but with freedom comes an inherent difficulty to impose any sort of regulatory structure on cyber-activity. Some have ventured so far to assert that the Internet has created a "totally unregulated data revolution," suggesting that the need for some sort of control is certainly a prevalent and well-recognized problem (Grauman 10). This lack of regulation manifests in many different forms, but most notably it gives Internet users a "no rules, no consequences" mentality. Under such circumstances, users often are not afraid to act more impulsively and aggressively than they would in their offline lives.

Through lack of regulation, a new online code-of-conduct has developed, a "cyber-morality" that bears little resemblance to what is considered acceptable behavior in everyday life. Online "comments sections" provide one small-scale example of the disparity between regular and cyber-morality. Comments sections, a popular website feature in which users can post reactions and messages, have become notorious breeding grounds for inflammatory and demeaning remarks and arguments. Additionally, a group called Freedom House, for example, determined that, in 2014, "the healthy treatment of women online" had declined "for the fourth year in a row" (Scola). The fact that such online behaviors tend to violate every aspect of conventional morality, and yet online they have become a ubiquity, demonstrates that the Internet's lack of regulatory structure has indeed fostered a new and caustic cyber-morality.

Cyber-morality not only alters the behavior of individual people, but that of nation-states as well: nations such as the United States, Russia, and China continually commit acts of cyber-warfare and espionage even in times of peace. The freedom and pervasive interconnectivity of cyberspace has provided nation-states with “a low-cost, high-payoff way to defend national sovereignty and to project national power” (Geers 4). By utilizing cyber-attacks, a new method of offense and intelligence-gathering, nations are able to efficiently wage an entirely new type of war: cyber war. Strangely, however, nations are almost constantly waging some form of cyber war against rival nations, even in times of definitive peace. For example, as recently as 2013, “Edward Snowden…published documents suggesting that the U.S. conducted cyber espionage against China,” and China hacked U.S. servers to obtain “access to proprietary information such as research and development data” from various governmental departments (Geers 9, 6). Were one of these nations to commit an act of conventional warfare, rather than cyber-warfare, against the other, a global crisis would ensue. Also, such an action would likely never even take place given today’s state of geopolitical relations. Thus, a critical question arises: why do nations commit such acts of cyber-warfare, and why do they go unpunished? The answer lies in the free and unregulated nature of cyberspace itself. Cyber war, “unlike the wars of yesteryear,…produces no dramatic images of exploding warheads;” similarly to the alternate morality found in Internet comments sections, cyberspace fosters its own warfare morality on the scale of nation-states (Geers 3). With no regulations or boundaries, nations are free to attack whomever they please, even when an equivalent act might be considered rash and overly aggressive outside the realm of cyberspace.

Nation-states’ willingness to commit acts of cyberwar provides a dangerous example of modern cyber-morality, and demonstrates that effectively unlimited freedom and lack of regulation serves as a great threat in cyberspace. Although the Internet’s free and open structure gives it many benefits, it also makes any implementation of control or regulation very difficult. The subsequent “do what I want” with impunity attitude adopted by internet users applies not only to individuals, but to nation-states as well. As the world’s largest nations, such as the United States or China, lose all sense of conventional morality and continue to commit cyberattacks, the dangerous potential of the alternate morality found in cyberspace becomes increasingly apparent. When will such attacks begin to escape from the realm of cyberspace and manifest in physical violence? Already, certain nations have employed cyberattacks to damage critical physical infrastructure (Geers 6, 13, 16, 18). The solution is obvious: there must exist more measures to filter what nations can and cannot do in cyberspace. While there have been significant improvements to cybersecurity in recent years, the issue of regulation warrants much more attention (Grauman 10). Clearly, we still have a long way to go in our quest for a secure and trustworthy future in cyberspace.

Works Cited

Geers, Kenneth, Darien Kindlund, Ned Moran, and Rob Rachwald. *World War C: Understanding Nation-State Motives Behind Today's Advanced Cyber Attacks*. Rep. FireEye, Inc., 2014. Web. 14 Feb. 2017. <http://cs.brown.edu/courses/cs180/static/files/lectures/readings/lecture1/World%20War%20C.pdf>.

Grauman, Brigid. *Cyber-security: The Vexed Question of Global Rules*. Rep. Security & Defence Agency, Feb. 2012. Web. 14 Feb. 2017. <http://cs.brown.edu/courses/csci1800/sources/2012_SDA_CybersecurityVexedQuestionGlobalRules.pdf>.

Scola, Nancy. "This was the Internet's worst, best year ever." *The Washington Post*. The Washington Post, 31 Dec. 2014. Web. 14 Feb. 2017. <https://www.washingtonpost.com/news/the-switch/wp/2014/12/31/this-was-the-internets-worst-best-year-ever/?utm_term=.6e2b07acad2c>.