Human-Computer Interaction in Cyber Espionage and Terrorism

Hacker Culture

The hacker group Anonymous is a collection of loosely associated individuals with a shared culture and set of ideals. Much like interactions offline, this culture is transmitted through the use of memes and exclusionary “in jokes” to identify individuals with one another. Instead of using signs denoting race, gender, and class, the members of Anonymous use intellectual property, ideas, to transmit cultural knowledge. Members are able to use these codes to identify one another, despite the fact that members do not know one another’s identities. At times Anonymous can be like a living organism, with disparate parts morphing into various iterations independently and without coordinated effort. At other times it can descend with razor-sharp focus onto a particular issue or cause.

Lulz Security, or Lulzsec, is one such sharply focused iteration. The members of Lulzsec began as members of Anonymous, and truly never left. Their hacktivist methods, ideals of freedom of information and expression, and culture of mischief and whimsy are all Anonymous traits. However, they act with greater abandon, and have received criticism from other members of Anonymous for some of their less-than-ethical operations. Groups like Lulzsec arise from the primordial ooze of Anonymous, because of the difficulty inherent in legally disrupting corrupt systems. The new and exciting medium of the internet allows for greater breadth of information sharing, and greater potential for effective protest.

The members of Lulzsec, just like Anonymous, believe they are fighting for freedom and justice, but their freedom to wage effective and disruptive protest is extremely limited. Anonymous has been stigmatized as a potential threat to cyber security, and online protest is sharply curtailed to only the non-disruptive, status quo maintaining variety. Lulzsec is one result of limiting freedom of expression until there is no room for disruptive protest. When protestors are criminals, protestors behave more criminally.

The absolute ease with which change can be affected over this new medium of the internet is jarring and can often create a feeling of unreality. So much so, that the European Conference on e-government considered it worth investigating whether cyber disruption is a gateway drug to attacking physical infrastructure (Holt, Kilger, Chiang, & Yang, 2012). The culture of computer screen interaction having originated for many in the form of video games makes it difficult to conceptualize online interaction as equally real and valid. It originated as fiction, so it has a tendency to feel more fictional and less real.

Educational programs geared toward helping children develop hacker skills could also have the side benefit of creating a less fictionalized narrative for online spaces. If online interaction is something one studies in school, it may seem more connected to the real world. Additionally, if these educational programs have a focus on real-life consequences for online missteps the line between real life and the internet can become more blurred. However, there is a thin line between education and state-sponsored ideological indoctrination.

In recent studies on cyber warfare, the term “patriotic” is used to describe simply a fact of political rather than ideological alignment. Those that perform attacks against a state that their state happens to be at war with are deemed patriotic, distinguished from such ideological and cultural alignment that exists in Anonymous and other hacktivists (Dahan, 2013). According to this modus operandi, patriotism consists of fighting the enemies of one’s state, no matter who they may be, rather than of standing up for an ideal regardless of whether one’s current government supports that ideal.

This viewpoint on what constitutes patriotism harkens back to the McCarthy era of suspicion. Voices that questioned the powers that be or the “American” ideals were staunchly shunned. Ruth Brown, for example, was a librarian that stood up for freedom of information, but continuing to stock her library with several controversial texts, as well as encouraging integration and stocking multicultural journals. She fought against the idea of the public library as a single voice of indoctrination and attempted to support critical thought and multiple perspectives. The unfavorable era for such behavior saw her ousted.

A single notion of what constitutes patriotism is a dangerous proposition, and simply aligning one’s sights unquestioningly on an enemy rather than an ideological stance sounds terrifying. Importantly, public libraries have the same responsibilities now as in the McCarthy era in maintaining multiple perspectives and viewpoints of discourse, and not falling victim to a single narrative. Anonymous is the epitome of an ideological stance from multiple perspectives. Maintaining freedom to protest both effectively and legally is an important and valuable service, and public libraries are one of very few institutions in a position to maintain effective resources using the newest information media.

References:

Dahan, M. (2013). Hacking for the homeland: Patriotic hackers versus hacktivists. 8th International Conference on Information Warfare and Security.

Holt, T., Kilger, M., Chiang, L., Yang, C.-S. (2012). Comparing civilian willingness to attack critical infrastructure on and off line. Proceedings of the European Conference on e-Government.