Human-Computer Interaction in Cyber Espionage and Terrorism

Lulzsec: Case Study Part 1

1. Libraries, privacy, and freedom

Despite the stark differences between the two, there is a broad gray area between the categories of hacktivism and cyber terrorism. Librarians embody information freedom and freedom of speech as they engage in public service for the greater good. We strive to enable activists to obtain information and engage in protest without fear of retribution. On the other hand, we value privacy, and do not want to encourage unlawful intrusions into protected information. We also uphold copyright law and personal property rights. We have a responsibility to enable the freedom of speech and information, while also not enabling illegal activity. The fuzzy gray line between the two means that a current discussion of ethical and legal standards and policies is every-changing, and the need to closely examine the implications for public service is ubiquitous.

If public library resources are able to be utilized for cyber warfare, the backlash could put the information freedom of every other patron at risk, as well as spark policy and law controversy and a debate about how much freedom libraries should really have. More limitations of freedom could be enacted for those citizens that are following the law, and protests of a certain type could become difficult or impossible to attempt privately. This is truly a scary proposition. It is not only the responsibility of libraries to not only hold the line on information freedom and attempt to advocate for greater privacy and freedom for average citizens. It is also the responsibility of libraries to ensure that such powerful public resources are not turned to harmful purposes.

There are some who say that privacy and anonymity are the antithesis of organized activism (real activism), but the work by Anonymous and especially Lulzsec seems to contradict that premise. The actors are willing to do dangerous things, which could lead to imprisonment, all for a powerful idea. Lulzsec members in particular are able to establish a rapport without the need for identifying information of any kind.

1. Lulzsec, an introduction

Lulz Security, or Lulzsec, is originally a small offshoot of the hacker group Anonymous. While Anonymous could not really be called an organization, but rather a shared idea or concept, Lulzsec is more focused grouping of individuals that could actually be labelled as an organization. They have a structure and division of labor like a true organization. However, they embody many of the ideals of Anonymous. They have a strong stance on freedom of speech and information, and are quick to attack anyone that seems to curtail either. However, “where Anonymous often trod the line between civil disobedience and criminality, Lulzsec blasted right through it” (Murphy, 2011, 46), Functionally, they are a group of people united by like-minded ideas, with the skills to plan and implement cyber-attacks to propagate those ideas. Rather than the fluid group of the Anonymous hivemind, Lulzsec is a more static, active, and secretive group.

From what we know about the individual members of Lulzsec, those whose identities are now known are young men, who in another era could have grown up to be Bill Gates or Steve Jobs. In the interviews they’ve given they carry themselves as socially awkward adolescent boys, with the intelligence and skills at using modern technology to its maximum effectiveness (royalcourttheater, 2014) Some less-than-ethical tinkering put them in a worldwide spotlight and earned them all jail time.

1. Lulzsec, the human aspects

Lulzsec engaged in several cyber attacks over an initial 50 day period during May and June 2011. The first attack was against the Fox Broadcasting Company in which Lulzsec released a data dump of the personal information of 73,000 contestants from the show X-factor. They then attacked Sony, stealing and releasing personal information of Sony accounts. Directly afterward, they attacked PBS, defacing their public site and posting fake news stories. Things got serious when Lulzsec took down the US CIA website, and the group gained some notoriety and fame. Lulzsec is credited with the shut-down of several other online games and organizations, some of which it denies, and received harsh criticism and backlash from its fellow members of the group Anonymous for disrupting systems that they regularly use. Lulzsec then declared war on several government websites, taking down UK’s Serious Organized Crime Agency and Brazilian government websites with the help of Anonymous, and seemed to come back into favor. It released information from the Arizona Department of Public Safety on policy and training manuals as well as personal identifying information on Arizona law enforcement officers (Lulzsec hacks).

On June 25, Lulzsec announced their retirement, as well as releasing several leftover bits of stolen data. However, they offered to come back with enough support from followers in Anonymous, and proceeded to hack into the Sun to post fake news stories and cause mayhem. After this, Lulzsec continued to occaisionally come together to hack various government and private company sites until the arrests and charges filed against many of the main coordinating members in July of the next year (Lulzsec hacks).

1. Lulzsec, goals

The stated goal of Lulzsec is “for the lulz,” basically meaning for amusement. They engage in hacking for their own benefit and amusement, and to stir up strong feelings. However, the motives are far more complex than stated. Lulzsec engaged in attacks on groups for political and ethical justifications, attempting to align their own agenda with that of Anonymous from whence they came. When they garnered too much backlash from the rest of Anonymous for attacking game sites with no idealogical standing, and criticism for their methods of releasing personal information of innocent bystanders, they were quick to fall back in line and begin working with Anonymous again and attempting to rebuild bridges. The political philosophy of Anonymous influences the actions of Lulzsec, so no discussion of motive can be complete without a discussion of Anonymous.

Lulzsec mainly chose its targets based on the principles of Anonymous: namely universal freedom of information and speech. They initially attacked Fox because of censorship policies, attacked Sony for its prosecution and policy toward other hackers, and attacked the Arizona police department over anti-immigration laws including racial profiling. However, many of their targets were also targets of convenience, truly attacked “for the lulz,” and chosen simply for the sake of availability. Lulzsec received criticism for a number of these attacks, both from within and without the hacker community.

One cannot discuss the ethics and morals of Lulzsec without contextualizing it with the ethics and morals of Anonymous, from whence Lulzsec sprung. Anonymous refers to itself as a hydra and also as a hivemind. Both descriptions are equally accurate and equally inaccurate. Anonymous is a hydra in that it has many heads which only multiply when one is destroyed. The idea is that is comprised of many identical units is flawed, because each head thinks for itself, and merely clings to the body out of a sense of belonging or similarity in principles. The hivemind analogy likewise leaves out the complexity of each mind thinking entirely for itself.

Anonymous does not have meetings to decide what to do, or any leadership, centralized or otherwise. “Anonymous is not a united front, but a hydra, a rhizome, comprising numerous different networks and working groups that are often at odds with one another” (Coleman, 2012, pp.B5). It has a generalized principle of freedom of speech and of freedom of information, as well as underlying sense of mischief and inappropriate amusement common to its culture. Every individual member has the freedom and right to interpret those principles for themselves, which leads to some controversial objectives. Lulzsec is one such controversial group, whose objectives are outside their principles for many members of Anonymous. (Knappenberger)

1. Lulzsec, public response

Lulzsec is a subject of controversy. Most agree that their methods went too far, and what they refer to as “collateral damage” is too severe to be written off their slate. However, others still see the ideals that inspired the attacks in a positive light, and see the attacks as hacktivism gone too far. The US and UK governments both investigated these attacks and arrested many of the key players.

For Anonymous, especially the splinter known as Lulzsec, the internet is the last bastion of freedom. Many forms of protest available in previous generations are reduced in effectiveness today. Sit-ins do not disrupt the way they once did, with so much of our daily activity done online. Online activity is a new front line for activism, because hackers can individually disrupt the status quo in ways that single individuals normally cannot. However, this new age is not without risks. Many believe that Lulzsec went too far in its revelations, giving out the personal information on innocent customers, which affected the innocent bystanders more than the companies and organizations attacked.

The main theme in the literature on hacking is the idea of duality, that “various actors and institutions can be both protectors and threats to privacy” simultaneously (Steinmets & Gerber, 2015, 35). Protest is inherently about performance. It’s about showing up the bad guy, and about being Robin Hood. “Transgressions…unravel the often oppressive force of norms, conventions and the law” (McQuillan, 2015, 570), and Anonymous has always been a fan of performance and bravado. The fact that Lulzsec made a leap from performance to acceptable collateral damage seems to be what made this group so notorious.

However, “violence either plays a part in constituting a new situation or is carried out by institutions trying to preserve the status quo” and Lulzsec “in a kind of ritual inversion of the operations of those companies, releasing their data to the public” (McQuillan, 2015, 571-2). They released information, paradoxically, from those companies most opposed to both privacy and the freedom of information. McQuillan (2015) argues that Lulzsec and other such hacker groups are side-stepping the democratic process of law because it has proved itself ineffective at encouraging real change. Cyber warfare is one of few available methods wherein small groups of people can cause enough disruption to encourage real change. And Lulzsec is nothing if not disruptive. The question is, whether their disruptions bring about positive change or negative.

References:

Coleman, G. (2012, February 21). Anonymous: Growing political force works in moral grey zone. *The Dominion Post*, pp. B5

Knappenberger, Brian. 2012. *We are legion: The story of hacktivists.*

Lulzsec hacks. (n.d.). Retrieved May 5, 2016 from the Know Your Memes Wiki: <http://knowyourmeme.com/memes/events/lulzsec-hacks>

McQuillan, D. (2015). Algorithmic states of exception. *European Journal of Cultural Studies,* 18(4-5), 564-576.

Murphy, S. (2011). Summer of lulz: How hacktivists have exposed the sorry state of internet security. *New Scientist*, 211: 2829, 46-49.

Royalcourttheatre. (2014, September 29). The big idea: In conversation with Lulzsec. [Video file] Retrieved from: <https://www.youtube.com/watch?v=KpGiLPF5BxQ>

Steinmetz, K., Gerber, J. (2015). “It doesn’t have to be this way”: Hacker perspectives on privacy. *Social Justice*, 41(3), 29-51.