Journal of
Theoretical & Philosophical Criminology

January/February, 2016

Understanding Cyber-Vigilantism: A Conceptual Framework

Joshua Smallridge, *Fairmont State University*

Philip Wagner, *University of Wisconsin-Parkside*

Justin N. Crowl, *Mansfield University of Pennsylvania*

Abstract

This article proposes a conceptual framework for cyber-vigilantism that proves useful for distinguishing it from other potentially harmful online actions. An overview of vigilantism is first presented, with particular attention given to Johnston's (1996) work, in which we use as a conceptual guide. Next, we discuss cyber-vigilantism along with several acts associated with this type of online activity. A number of cases involving vigilantism are identified and discussed. Through this analysis, a definition of cyber-vigilantism is developed that we argue is conceptually distinct and applicable to a wide range of contemporary online behaviors. Finally, future research considerations are offered to conclude.

Introduction

The introduction and proliferation of the internet has created vast opportunities for advancement in areas such as entertainment, commerce, and communications. We are now more connected with each other and the world around us than ever before. This greater connectivity, however, does not come without limitations. Over the last few years, acts classified by the media as online vigilantism have begun to attract public attention.

This is not surprising, as the vigilante is a figure that often captures public imagination. There are numerous examples which have held media attention over the last century or so. In November of 1933, one of the largest public acts of vigilantism in American history occurred in Los Angeles, when two kidnappers were lynched with live radio coverage. Later, these individuals were pardoned by the Governor of California (Murphy, 2010). Another notable case occurred in 1981 and involved the death of Ken McElroy, who had participated in crimes ranging from rape and arson to multiple shootings. McElroy shot in front of 47 witnesses by a vigilante shortly after the sheriff drove out of town. Despite multiple witnesses, no one was ever charged in McElroy's murder (Sulzberger, 2010). An additional example mirrors the plot of the film *Death Wish,* which aired in 1983. One year later, Barnhard Goets opened fire on a group of youth who attempted to mug him on the subway. Despite an admission that his actions went beyond self-defense, Goets was acquitted on all counts and only served eight months for an unlicensed firearm (Johnson, 1987). With examples such as these, it could be argued that the vigilante has always been a popular figure. Despite this considerable public interest, scholarly research and scientific discourse on cyber-vigilantism has been limited.

While vigilante activity has fascinated some, it has become a very serious concern for others. Compounding this reality is the fact that vigilantism has been only sporadically examined over the last few decades within the criminological discipline. In this article, we develop a conceptual definition of cyber-vigilantism through guidance of the conceptual framework of past studies on vigilantism. In particular, we use the definition of cyber-vigilantism developed by Johnston (1996) as a basis for our analysis. We then expand on this definition through the introduction and analysis of numerous cases involving vigilante activity. In doing so, a definition of cyber-vigilantism emerges that we argue better applies on a conceptual basis to a wide range of online behaviors.

Vigilantism Defined

The term vigilante is of Spanish origin, meaning 'watchman' or 'guard'. It has its roots in the Latin word vigilans (Merriam-Webster, 2015). There have been numerous definitions of vigilantism developed over the years. More often than not the term is used very loosely or in a sensationalized manner, particularly by the media (Johnston, 1996). Even within academic circles, there is considerable disagreement regarding what constitutes vigilantism (Marx & Archer, 1976; Rosenbaum & Sederberg, 1976). In this section, various contested issues in the conceptualization of vigilantism are discussed.

Johnston (1996) developed what is likely the most thorough definition of vigilantism to date, and for this reason, his definition will be used as a guide. Johnston defines vigilantism as "a social movement giving rise to premeditated acts of force - or threatened force - by autonomous citizens" (p. 232). Vigilantism arises as a response to the breaking of norms by individuals and groups. In addition, vigilantes often seek to provide crime control, social control, and an assurance of security to themselves and those of the social order they seek to serve.

Six elements are necessary, according to Johnston (1996), for an act to be considered vigilantism. These elements serve to differentiate vigilantism from other acts that are often misleadingly given the vigilante classification. First, there must be at least a minimal level of planning, premeditation or organization by the person responsible for the act. This caveat removes spontaneous interpersonal conflict from consideration as vigilantism. Thus, an individual who, in the absence of planning, defends him/herself against an assailant should not be considered a vigilante.

We share this assertion with Johnston; without this element, vigilantism would become too broad of a concept.

The second necessary element of vigilantism identified by Johnston (1996) is that the act must be undertaken by private agents unaffiliated with law enforcement. An agent of the state nor a public institution, therefore, can be classified as a vigilante. This is counter to the definition of vigilantism advanced by Rosenbaum and Sedeberg (1976), which included actions by on and off duty police officers. Johnston argued that a law enforcement officer cannot engage in vigilantism, as officers still maintain their police powers when off duty. We only partially agree with Johnston on this element of vigilantism. Moreover, the third element Johnston (1996) identifies is that the act must be autonomous and free from state support. Stated alternatively, the act should not be sanctioned by the government, particularly agencies in the criminal justice system. We have retained this element unaltered for our own definition. Thus, on the second and third points, an agent of law enforcement who is off-duty and acting outside the sanction of the government while online should be considered a vigilante due to lack of governmental support.

The fourth element focuses on the type of harm done by the act in question. Utilizing Johnston's conceptualization, for an act to be considered vigilantism, it must encompass the use or threatened use of force. While this is perhaps one of the most crucial elements to Johnston's conceptualization, it may also be the most limiting when specifically applied to online vigilantism. While the threatened use of force is possible, actual physical force, which involves violence, is seldom a byproduct of online vigilante activities. To this end, we argue that the focus of vigilantism should be broadened so as to encapsulate the causation of harm. This harm should arises from a credible threat or source. The reasons for this change are discussed in the conclusion section of this article.

A related issue is whether the vigilante activity needs to be criminal in nature. Many authors recognize both legal and illegal forms of vigilantism (Johnston, 1996; Resenbaum & Sederberg, 1974), while others only recognize illegal forms (Haas, 2010). Vigilantism in itself is not a crime, meaning there is often no statute specifically against taking the law into one's own hands. Of course, a person who embarks down this path can be held culpable if their behavior violates the criminal law. The definition of vigilantism as advanced by Haas (2010) only focused on illegal actions, excluding citizen arrests and self-defense. We support the claim that acts of self-defense should not be considered as vigilante experiences. However, like Johnston, we recognize the existence of both legal and illegal forms of vigilantism.

The fifth element of vigilantism, according to Johnston (1996), requires the vigilante experience to be in response to a criminal or socially deviant action that is a transgression of institutionalized norms. The transgression can be either real or perceived. This requirement that the act is a transgression of institutionalized norms is important because it limits the range of behaviors that can be considered vigilantism. The final two elements focus on the goal or motivation of the vigilante. For an act to be considered vigilantism, the goal of the action must be to control crime or other social infractions, specifically done by offering assurances of personal and collective security to people of the appropriate social order. This concept of security is vital, according to Johnston (1996), in that it helps to link the autonomous aspect of vigilantism with the reaction to social deviance element.

What is Cyber-Vigilantism?

Like with traditional forms of vigilantism, society has cast a wide net in labeling actions as cyber-vigilantism. Some of the activities labeled by the media as cyber-vigilantism include, but are not limited to, scam baiting (Andrews, 2006), acts described as hacktivism (Coleman, 2011), citizen led cyber-stings, such as those orchestrated by Perverted Justice (Schultz, 2004), and crowdsourced acts of vigilantism. The latter concept involves individuals contributing their individual efforts toward a common goal, a phenomenon often described as “the human flesh search engine” in China (Cheong & Gong, 2010; Skoric, Chua, Liew, Wong & Yeo, 2010). This is the term used to describe the crowdsourced actions of Chinese netizens who see a form of outrage and then use the internet to punish the offender by posting personal details ranging from phone number and address to blood type online for individuals to view and use in harassment. The “human flesh search engine” being used to persecute those who have caused perceived harm is similar to the American website 4chan, where all posts are anonymous in nature, which is known for incubating a number of memes found across the internet, but also for its users gathering together behind causes. One particular case involved the users of the service exposing a cat named Dusty’s abuser to his local police department (Dewey, 2014).

Such crowdsourced vigilante activities generally take two forms. These forms, which are not always mutually exclusive, include (1) mass retributive actions against an identified wrongdoer, and (2) collective attempts to solve real life crimes. The aforementioned vigilante activities are not exhaustive; it is possible that other acts can be considered cyber-vigilantism. In the following sections, a concise overview of scambaiting, hacktivism, citizen lead cyber-stings, and crowdsourced vigilantism is provided. We then integrate and synthesize numerous cases that are specific and applicable to each vigilante activity. In doing so, we construct a more contemporary definition of cyber-vigilantism that distinguishes it from related activities such as cyber-harassment and bullying.

Scam baiting

Internet scams distributed through email have put a new face on an old problem. Perhaps the most prevalent scam clogging email accounts around the world is the Nigerian ‘419’ scam. There are many variants of this scam. In general, the scammer, or a series of bots which have been programmed to take the initial role of the scammer to send out mass quantities of these messages, portrays themselves as someone with a great deal of money that needs to transfer the money through a trusted bank account. The target of the scam is promised a significant amount of the money if they allow the funds to be transferred through their personal bank account. The money, in reality, does not exist. Once the intended target shows interest, the con artist may inform them that they will need a small sum of money to cover fees or circumvent an impending problem, with reassurance that the final payout will greatly outweigh any costs that were accrued. The con artist will then keep fabricating obstacles to coerce money from the target for as long as possible (Tuovinen & Röning, 2007).

Scam baiting has developed as a countermeasure to 419 and similar email scams, the most recognized of which contains an offer of financial gain from a Nigerian prince. Assuming a fake identity of their own, scambaiters portray themselves as an unwitting target, typically done for amusement reasons or civic duty engagement, or both. In an effort to identify and publicly expose the scammers, the baiter will first reply to a scam email and pretend to be interested in the scam. In doing so, the baiter will try to waste the scammer’s time and other resources for as long as possible. To the extent possible, the baiter may also collect personal information about the scammer to turn over to authorities (Tuovinen & Röning, 2007). In this context, scambaiters counter deceit with deceit.

While scam baiting may seem harmless, the consequences of such an activity should not be overlooked, as harm could be a very real consequence. Scambaiters often provide addresses for the shipment of items or fail to use a proxy with a traceable IP address. As a result, it is possible for scambaiters to be tracked down and potentially harmed by those individuals they are costing money, time, and resources. In the face of such possibilities of harm, should scambaiters, then, be considered online vigilantes?

Hacktivism

Prior to discussing hacktivism, information that provides a foundation for understanding this type of behavior is reviewed. First published in the ezine Phrack in 1986, the Hacker Manifesto by The Mentor captured the foundation of hacker culture at the time. In the Manifesto, the Mentor laments the quality of schooling he received and extols the sense of discovery found in computers. The Manifesto also illustrates the antiestablishment idealization of much of the hacker community. The Mentor states:

> This is our world now… the world of the electron and the switch, the beauty of the baud. We make use of a service already existing without paying for what could be dirt-cheap if it wasn't run by profiteering gluttons, and you call us criminals. We explore… and you call us criminals. We seek after knowledge… and you call us criminals. We exist without skin color, without nationality, without religious bias… and you call us criminals. You build atomic bombs, you wage wars, you murder, cheat, and lie to us and try to make us believe it's for our own good, yet we're the criminals. (Mentor, 1986)

Although written more than 30 years ago, the Hacker Manifesto is still relevant today. The antiestablishment mentality is readily apparent in most acts of hacktivism.

Hacktivism is a combination of the terms hack and activism. The term, which lacks definitional lucidity, was created by members of the hacking group Cult of the Dead Cow (cDc). Oxblood Ruffin, a member of the cDc, defined hacktivism as something that "uses technology to improve human rights. It also employs nonviolent tactics and is aligned with the original intent of the Internet, which is to keep things up and running. With regard to tactics, things like DDoS attacks, Web defacements, malware, and network breaches are off limits (Allnitt, 2011, p. 2)." In this conceptualization, hacktivism is viewed as having a nonviolent connotation; however, it is often associated with more harmful forms of protest today.

Case 1 A prominent early example of hacktivism occurred during the summer of 1998 when hackers affiliated with the groups Milw0rm and Ashtray Lumberjacks carried out the largest ever mass attack on websites up to that time. They were able to do this by gaining access to the databases of a web-page hosting company called EasySpace. Users who tried to go to a webpage affected by the hack were instead redirected to a webpage displaying an anti-nuclear weapon message and a call for peace. Prior to that, members of Milw0rm had gained access to the servers of Bhabha Atomic Research center in India where they downloaded information and deleted some data from the servers (Hu, 1998). Both of these attacks were carried out in protest of continued proliferation of nuclear weapons in the world after India and Pakistan declared themselves nuclear powers.

The methods and motives of self-proclaimed hacktivists vary widely. Many groups and individuals may be considered hacktivist. However, the most prominent hacktivist group in recent years is Anonymous. Providing a simple definition of the group is an arduous task, as its name is manifested to coordinate a wide range of diverse actions (Coleman, 2011). This difficulty is compounded by the decentralized nature of the group which has no hierarchical structure. In fact, any individual or group could claim to represent the group. To this end, the group's activities have been attributed to a wide range of attacks and activities, ranging from pranks to political activism. Although hacktivist groups can engage in cyber-vigilantism, not all of their actions can be classified as such. Consider the following cases.

CASE 2. Members of Anonymous released the information of a 14 year old teen who created the website nocussing.com. After his personal information was released, the teen received thousands of threatening emails along with fictitious orders for pizza and pornography. This case carries many of the hallmarks of an attack motivated by the "lulz", which is a twist on the popular acronym lol (laughing out loud). The term is often used to express a motivation based on personal entertainment.

CASE 3. In January 2013, a group claiming to be Anonymous hacked the United States Sentencing Commission website, replacing the homepage with an embedded YouTube video entitled "Anonymous Operation Last Resort". The attack was in response to the suicide of Aaron Swartz, who two years prior was arrested and charged with two counts of wire fraud and multiple violations under the Computer Fraud and Abuse Act often referred to as the hacking statute (Brumfield, 2013). The charges mounted against Swartz carried a maximum penalty of 35 years in prison. The video posted on the Sentencing Commission's website criticized the application of the federal law in the Swartz case as "highly disproportionate" (Anonymous, 2013). On the video, the attackers threatened to release encryption keys to various files containing sensitive government information.

CASE 4. In October 2011, Anonymous launched "Operation Darknet", which was a code name for a series of attacks against child pornography sites accessed via the TOR network (Stone, 2011). The TOR network was built to allow internet users in repressive regimes to anonymously use the internet. However, criminal enterprises have also benefited by the increased anonymity offered by the service. In addition to child porn, the service has been used to set up online drug marketplaces such as the "Silk Road" and illegal weapon marketplaces such as "The Armory". The structure of TOR is decentralized; as such, many hidden services on the TOR network serve as a listing for other websites such as the Hidden Wiki (Tor Project, 2015).

Anonymous began their attack by removing links to child pornography from the Hidden Wiki. Soon after their attack, Anonymous members began to target the Freedom Hosting, whose servers hosted many of the child porn sites linked to by the Hidden Wiki. After identifying Freedom Hosting as the source of many of the child porn sites, Anonymous members sent a warning to the company to remove the content. When Freedom Hosting did not comply, Anonymous initiated a distributed denial of service (DDoS) attack on their servers (Leyden, 2011). This type of attack involves multiple virus-infected systems that are used to maliciously target a single system through a distributed viral attack. The group then focused their attack on a particular child porn site, Lolita City, by releasing the usernames and activities of 1,589 users of the site (Gallagher, 2011). Their final attacked released the IP addresses of nearly 200 users who had accessed the child porn section of the Hidden Wiki (Liebowitz, 2011).

The preceding cases elucidate the varying nature of attacks attributed to Anonymous. It is quite clear that group's identity has evolved over time (Gabriella, 2011), particularly as it demonstrates a penchant for campaigns designed to prank or troll targets. Such motivation was particularly pronounced in early attacks by the group on Scientology. Since this time, the group has continued to focus much of their activities on political and social causes that can be identified as hacktivism. But can these activities, ranging from pranks to high profile hacktivism, of Anonymous and other hacktivist groups be classified as cyber-vigilantism?

Crowdsourcing for Justice

There are multiple forms of behavior labeled as vigilantism that rely on crowdsourced expertise in response to societal wrongs, both real and perceived. These incidents of crowdsourced civilian involvement can be categorized by the level of organization exhibited by the individuals participating in the justice seeking activities. On one hand, there are relatively organized civilian groups that rely on the expertise of initiated volunteers to carry out their activities. In contrast, there are short-lived groups that mobilize in response to a particular injustice or social wrong. It is to these areas we now turn.

Organized Crowdsourced Activities

Well-organized civilian groups, like Perverted Justice, engage in a variety of activities to identify criminals, particularly pedophiles, who operate online. These groups are commonly recognized for the sting operations they conduct to expose online child predators, as depicted in the NBC show “To Catch a Predator” (Hansen, 2004). In these operations, members of the group pose as juveniles online using various forms of communication, such as an IRC chat channel, in which a pedophile may try to make contact with children. Upon contact, group members will work to collect incriminating evidence in the form of chat logs on the offender. The information obtained will then often be provided to law enforcement in hopes that the perpetrator will be held criminally responsible for the incident (Perverted Justice, 2008).

A distinction can be made regarding how Perverted Justice operated before and after its 100th conviction. Prior to the 100th conviction, chat logs and offender information would be posted to the Perverted Justice website even if law enforcement decided not to pursue a case. After the 100th conviction, the site policy was changed so that only cases with law enforcement support would be posted (Perverted Justice, 2006).

Although groups like Perverted Justice pursue criminals online, we contend that in most cases they should not be considered vigilantes because their actions are legitimized by the state through the support of law enforcement. Such groups work in tandem with law enforcement agencies to identify and capture child predators. In general, the volunteers with Perverted Justice will do most of the leg work leading up to a child predator sting operation. However, they turn the evidence they have collected over to the police for them to arrest the offenders they identify and capture. Thus, their actions should generally not be considered cyber-vigilantism if we apply Johnston’s (1996) criteria. However, if law enforcement support is not obtained, such as in the early days of the group, their actions could be considered vigilantism if all other criteria are met. It is clear from an examination of the history of Perverted Justice that individuals and groups can potentially drift between vigilantism and proactive citizenship.

Spontaneous Crowdsourced Activities

In addition to well-organized civilian groups, there are ephemeral groups who mobilize in response to a perceived wrong or injustice. These groups generally dissipate quickly as the initial furor of the initiating event fade into memory. Such groups generally materialize in loosely controlled online communities such as 4chan (Huey, Nhan & Broll, 2012). Deemed the ‘Human Flesh Search Engine’ by the People’s Republic of China (Skoric et al., 2010), this phenomena brings together individuals with the goal of tracking down those who have committed acts which may not be illegal but are found to violate the norms of society. Once these people are found by their fellow online citizens, their information is publically posted to shame and possibly intimidate the offending individual from further transgressions (Cheong & Gong, 2010). Consider the following cases.

CASE 5. One of the more prominent cases involving spontaneous crowdsourcing gained international attention in 2010 with a pair of university students in Beijing committing a hit and run at Hebei University. At the time of the incident, a drunk driver hit two female students who were rollerblading. One of the students suffered a fracture in her left leg and the other student died the next day after being thrown through the air by the impact. The driver was Li Qiming, who shouted as he drove off, “Sue me if you can, my father is Li Gang” (Wines, 2010).

Li Gang, it was later confirmed, was the deputy director of the Baoding City Public Security Bureau and the father of Li Qiming (BBC News, 2011). Many on campus were angered by the indifference that Li Qiming showed after injuring the two young women. Outrage mounted, and as a result, details of his life began to be posted online by those seeking justice. Dozens of students and teachers held a candlelight vigil for the dead, and by the time the crowd had dispersed, more than 400 people had gathered (Xiao, 2010). This vigil was the beginning of a new groundswell in the human flesh search engine as students became angrier at the perceived attempt to invoke the authorities as protection against the commission of a crime.

CASE 6. A massive earthquake struck Sichuan, a province of China, in 2008 and left over 350,000 injured and almost 70,000 dead. Gao Qianhui, a resident of the Liaoning province in northeastern China, posted a video on the popular website YouTube, in which she complained about the nationwide mandatory three day mourning period (Lemon, 2008). She expressed no sympathy for the victims and instead was outraged that the government had stopped her television programs and impeded the ability of Chinese citizens to play online games during that period. Shortly after the video was posted, the human flesh search engine emerged and details about the woman, apparently misidentified as Zhang Ya, began to appear online. This information ranged from her online usernames to other personal information along with letters of apology that were purportedly from her family. As a result of the incident, Gao was placed into custody days later by Chinese civil authorities for unmentioned reasons (Tan, 2008).

CASE 7. A female student, identified as Xiong Jiaquing, attacked another woman in an alleyway in Shanghai, apparently in response to a fight over a boyfriend, in which the victim refused to fight back. This attack was videotaped and uploaded to the internet the same night it occurred (Fauna, 2009). The seemingly unprovoked attack outraged internet users, prompting some people to post online the attacker's personal information, including her age, home and campus address, and home telephone number (Fauna, 2009). Hateful comments were also posted about the transgressor, and a demonstration of over 200 people gathered to protest the attack.

CASE 8. A young woman named Bi Jiao was driving in Jiyuan when her side mirror struck a ten year old girl in the face (Boehler, 2013). Rather than ask the girl if she were okay and needed help, Jiao instead chose to berate the girl's mother for allowing her child to be so close to the street. When angry onlookers began to gather, she reported exclaimed, "I come from an influential family" (Tao, 2013). The public security department in Jiyuan was quick to use its microblogging site to release personal information on Jiao, precisely stating that she was not a person of influence, contrary to her claim. Chinese netizens expressed unrelenting anger toward the incident and disbelief that something like this occurred (Boehler, 2013).

These cases involving spontaneous crowdsourced activities are fitting to be labeled cyber-vigilantism. Admittedly, many of these acts gain state sanction ex post facto; however, this is not the same as working in concert with the authorities as in the case with Perverted Justice. The incident with Qiming (case 5) should be considered vigilantism until such time as the authorities became involved after realizing the outcry was not lessening, at which point the crowd became pseudo-state sanctioned. Similarly, the incident involving Jiao hitting the young girl with her car (case 8) can be considered a vigilante activity, particularly under Johnston's definition, with the inclusion of the threats of violence and death. However, the state moved quickly to use a police microblogging service to release copious amounts of information about the woman to the public, undercutting their own dissemination of personal information that would be utilized for the purposes of coordinating or supporting violent action taken against her.

Cases 6 and 7, which involved the threat of force to right a perceived wrong against society, would fit well within Johnston's definition of vigilantism. Recall that both cases involved the emergence of the human flesh search engine, with autonomous citizens in each case becoming outraged as a result of a perceived injustice. In an effort to help control the situation, the personal information of each transgressor was posted online. Threats of violence and potential harm immediately followed. We argue that the cases also fit within our conceptual basis of cyber-vigilantism. Actual physical force and violence were not a direct byproduct of the online vigilante activity in both cases; however, the threat of force and potential violence was evident, with harm being caused from credible sources.

Conceptualizing Cyber-Vigilantism

As evidenced in the literature, there have been few serious attempts to conceptualize vigilantism and even fewer attempts when cyber-vigilantism is considered. This is particularly surprising, given the recent concern for online vigilante activity and the costs incurred from this phenomena. In the following section, a conceptualization of cyber-vigilantism is developed, which expands on the foundation laid by Johnston (1996). We contend that portions of the six elements of vigilantism articulated by Johnston must be altered to reflect the new reality of vigilantism created by the emergence of the internet.

To review, for an act to be classified as vigilantism under Johnston's conceptualization, the following six elements must be met. First, at least minimal planning, premeditation, and organization must take place. Second, the act must be carried out by private agents. Third, these private agents must not have support or authority granted to them by the state. Fourth, the act must include the use of force or threat of force. Fifth, the motivation behind the act must be a response to perceived crime or social deviance. Sixth, the goal of the act should be to provide assurances of safety. Johnston summarized this as follows:

> ...vigilantism is a social movement giving rise to a premeditated acts of force -- or threatened force--by autonomous citizens. It arises as a reaction to the transgression of institutionalized norms by individuals or groups--or to their potential or imputed transgression. Such acts are focused upon crime control and/ or social control and aim to offer assurances (or 'guarantees') of security both to participants and to other members of a given established order (p. 229).

Most of the cases reviewed in the preceding sections would not be considered vigilantism under Johnston's definition. With some alterations, though, the definition becomes more contemporary and applicable for distinguishing cyber-vigilantism from other forms of cyber-deviance such as cyber-harassment, cyber-bullying, and acts of political activism. The first three requirements for vigilantism created by Johnston (1996) apply equally well for distinguishing acts of cyber-vigilantism from other online deviance as the original definition did with traditional forms of vigilantism. However, a few modifications are needed for the second requirement. We disagree with Johnston in his assertion that off duty officers cannot engage in vigilantism. Rather than drawing a hard line in the sand, it is more useful to make a distinction between officers acting in and outside of their policing role. If an officer confronts a criminal and makes an arrest, they are not acting as a vigilante regardless of whether they were on duty at the time. To the contrary, if officers step away from their official role and act outside of the limits of the legal system, their actions can be considered vigilantism. This is especially true with cyber-vigilantism where an individual's identity can be shrouded in anonymity.

With our modification, the application of the first three criteria helps narrow the actions that may be considered cyber-vigilantism. For example, many of the activities to identify and incriminate child predators online performed by groups like Perverted Justice should generally not be considered vigilantism because they are state sanctioned through cooperation with law enforcement. Similarly, actions such as those in the Li Gang incident (case 5) fall short of being classified as cyber vigilantism, particularly due to the intervention and dominance of governmental authorities in dealing with the perceived injustice of the event.

The fourth element that Johnston (1996) mentions is problematic in creating a conceptualization of online vigilantism, as physical violence is rarely a component of digital attacks. Some activities labeled as cyber-vigilantism could still satisfy Johnston's fourth element through the threat of violence if not actual violence. For example, the actions taken by Anonymous under Operation Darknet (case 4) could still be classified as vigilantism due to the overt physical threats made in the video they released on Youtube. In the video, the group articulated their desire to make the darknet an inhospitable place for child pornographers by creating "fear of persecution or death". However, retaining this aspect of Johnston's definition unaltered would exclude many incidents commonly defined as cyber-vigilantism, thereby limiting the scope of the definition to one that is too narrow to be of use.

The activities carried out as part of Operation Darknet meet all of the elements of Johnston's definition of vigilantism. However, if we were to remove the threat of death articulated in the Operation Darknet video, would it be right to no longer consider this an act of vigilantism? Even if the threat of death were removed, other types of harm were apparent in this case. Applying the definition of cyber-vigilantism to scambaiters raises the same questions. The activities undertaken by scambaiters rarely lead to physical violence or the threat of violence. However, the scammer usually experiences some form of retributive harm from the baiter. It is clear that to have a more practical definition of cyber-vigilantism, the requirement of physical violence or threat of violence should be modified by changing the requirement to the causation of harm or threat thereof. This would allow the inclusion of many non-physical mechanisms of harm (e.g., DDoS attacks, website hacking and defacement, the release of personal or sensitive information, and the destruction of virtual property) that are often the hallmark of online attacks. It would also allow acts of scambaiting to be defined as cyber-vigilantism if the scambaiter engages in a counter scam to cause some type of harm to the original scammer.

As mentioned previously, there is some disagreement in the literature regarding the perceived need for an act of vigilantism to violate the law in some way. While most acts of vigilantism involve some form of criminality, it is not a required feature. This is especially true when cyber-based attacks are taken into account. The law, as it relates to cybercrime, is constantly evolving. Many harmful acts that can be carried out online are not sufficiently covered by legal principles. A good example of this deficiency is online harassment as seen in many crowdsourced attacks. Although the act of online harassment clearly causes harm to the victim, the specifics and modality are not always illegal. In addition, the law can vary drastically between jurisdictions. For these reasons, the classification of an act as cyber vigilantism should be based on the qualities of the act rather than its legality.

The fifth and sixth elements of Johnston's definition are vital when determining whether an act can be considered cyber vigilantism. Recall that an act of vigilantism must be focused on social or criminal control with the intention of offering reassurances of security to group members or a target audience. Therefore, it is the motivation of the actor that distinguishes these actions. This requirement is important for distinguishing acts of online vigilantism from other acts of social harm carried out online such as cyber-bullying and more general acts of harassment. According to Citron (2014) "…cyber harassment is often understood to involve the international inflection of substantial emotional distress accomplished by online speech that is persistent enough to amount to a "course of action" rather than an isolated incident" (p. 3). In this respect, cyber-bullying can generally be viewed as a subset of cyber-harassment. Although acts of cyber vigilantism can involve harassment, it is not a definitive feature of the act. In cases of cyber-harassment, the motivation behind the attack must be examined to determine if an action should be considered vigilantism.

To recap, this section expanded the definition of vigilantism provided by Johnston (1996), thus making it compatible with vigilante actions occurring through cyberspace. As we have demonstrated, the majority of Johnston's definition remains applicable to cyber-vigilantism, serving as a sound conceptual basis for distinguishing cyber-vigilantism from other malicious activities that occur in online communities. However, we maintain that some elements need to be altered. For instance, one element was the requirement that the vigilante action result in physical violence or the threat thereof. By extending the definition to allow for a broader spectrum of harm, we arrive at a definition that is broad enough to apply to a wide range of online behaviors but specific enough to still allow for meaningful distinctions to be drawn.

For an act to be considered cyber vigilantism, it must satisfy all six of the requirements we have outlined in the preceding pages. A number of distinctions can be made when the definition of vigilantism is taken as a whole. For example, a white hat hacker would not be considered a vigilante because the act is not motivated by a desire to exert criminal or social control. In addition, legitimate cases of self-defense would not be considered vigilantism as the motive is immediate self-preservation rather than retaliation against crime or social deviance. In the digital realm, the concept of self-defense is an area of significant disagreement. This is especially true when considering the Cybersecurity Information Sharing Act of 2015 (CISA), which recently gave companies the legal authority to engage in "defensive measures" against online threats (Library of Congress, 2015). There is currently a great deal of uncertainty regarding what these "defensive measures" would entail (Nojeim & Butler, 2015). A full discussion of the appropriateness and limitations of the countermeasures authorized in the act is beyond the scope of this paper, as the current definition of "defensive measures" appears to be nebulous and little agreed upon in discussion of that bill.

Where Do We Go From Here?

Vigilantism is a topic in need of greater criminological analysis. To date, very little empirical research has been conducted on the topic. Unfortunately, Johnston's (1996) call for vigilantism research has went largely unheeded. This is a fact that remains true for traditional forms of vigilantism as well as newer forms occurring in cyberspace. There is still a great need for further research with both variants of vigilantism, and it is our hope that the call for further online vigilantism research does not suffer the same ignominy.

The conceptual basis for online vigilantism presented herein provides a foundation for multiple lines of inquiry for future research to pursue. First, more research needs to be conducted on the activities of hacktivist groups. This is an area of study that has already attracted much attention. For example, Coleman (2014) conducted an in-depth examination of the hacktivist group Anonymous, charting the evolution of the group over time and highlighting its many faces. As noted earlier, hacktivist groups participate in a wide range of behaviors online. Some of these behaviors should be considered vigilantism while others should not. This distinction is largely based on the motivation of an attack. Making a distinction between hacktivist operations based on motive will allow deeper analysis and comparison of hacktivist operations and groups.

Future research should also examine the social factors at play in instances of spontaneous and organized crowdsourced vigilantism. A qualitative paradigm would likely serve best in this regard, either through a case study approach or observational research. It would be particularly useful to examine the social mechanisms at play in the spread of spontaneous instances of crowdsourced vigilantism through direct observation of websites where it often foments, such as 4chan or Reddit. There are communities on both sites, which are known for their history of engaging in targeted activities against those who have been accused of perpetrating harm.

In the event of discovering the occurrence of vigilantism, it would be particularly worthwhile to analyze discussions of the activity. Content analyses of the comments could reveal a dearth of information regarding the motivations behind the action and the rationalizations for those who are engaging in it. It would also allow for the construction of a model timeline regarding the action from its inception to reaching a critical mass where the actual crowdsourced vigilantism begins. Future research should examine public perceptions of various forms of cyber-vigilantism as well as ethical considerations of the subject. In doing so, a deeper conceptual understanding of cyber-vigilantism will continue to emerge and factors associated with its occurrence can be identified and subsequently addressed. And finally, future research should consider the applicability of the conceptualization of vigilantism as outlined in this article for traditional forms of vigilantism as well as cyber vigilantism. Our definitions fit particularly well for western societies with a capitalist system and well-structured legal systems. However, we concede that it may not fit perfectly for all societies. It would be worthwhile to examine the concept of vigilantism across multiple systems of justice. One specific area of focus could be the comparison of societies based on what constitutes "state support".

References

Allnitt, L. (2011). Old-school hacker Oxblood Ruffin discusses anonymous and the future of hacktivism. *Radio Free Europe Radio Liberty*. Retrieved from http://www.rferl.org/content/hacker_oxblood_ruffin_discusses_anonymous_and_the_future_of_hacktivism/24228166.html

Andrews, R. (2006). Baiters teach scammers a lesson. Wired. Retrieved from http://www.wired.com/techbiz/it/news/2006/08/71387

Anonymous (2013). Anonymous Operation Last Resort. Retrieved from http://www.youtube.com/watch?v=WaPni5O2YyI

BBC News (2011). China hit-and-run driver sentenced to six years in jail. Retrieved from http://www.bbc.co.uk/news/world-asia-pacific-12317756

Boehler, P. (2013). Pictured: Henan residents on rampage over Honda driver's sense of entitlement. *South China Morning Post*. Retrieved from http://www.scmp.com/news/china/article/1247402/pictured-henan-residents-rampage-over-honda-drivers-sense-entitlement

Brumfield, B. (2013). Anonymous threatens Justice Department over hacktivist death. *CNN News.* Retrieved from http://www.cnn.com/2013/01/26/tech/anonymous-threat/index.html

Cheong, P. H., & Gong, J. (2010). Cyber vigilantism, transmedia collective intelligence, and civic participation. *Chinese Journal of Communication,* 3(4), 471-487.

Citron, D. K. (2014). *Hate crimes in cyberspace*. Cambridge, MA: Harvard University Press.

Coleman, G. (2011). Anonymous: From the lulz to collective action. *The New Everyday: A Media Commons Project.* Retrieved from http://mediacommons.futureofthebook.org /tne/pieces/anonymous-lulz-collective-action

Coleman, G. (2014). *Hacker, hoaxer, whistleblower, spy: The many faces of anonymous*. Brooklyn, NY: Verso.

Dewey, C. (2014, September 25). Absolutely everything you need to know to understand 4chan, the internet's own bogeyman. *The Washington Post.* Retrieved from https://www.washingtonpost.com/news/the-intersect/wp/2014/09/25/absolutely-everything-you-need-to-know-to-understand-4chan-the-internets-own-bogeyman/

Fauna (2009). Shanghai schoolgirl beating and human flesh search. Retrieved from http://www.chinasmack.com/2009/videos/shanghai-schoolgirl-beating-human-flesh-search.html

Gallagher, S. (2011). Anonymous takes down darknet child porn site on tor network. Retrieved from http://arstechnica.com/business/2011/10/anonymous-takes-down-darknet-child-porn-site-on-tor-network/

Haas, N. (2010) Public Support for Vigilantism. Amsterdam/Leiden: NSCR.

Hansen, C. (2004). To catch a predator [Television series episode]. In N. Shapiro (Producer), *Dateline*. New York, NY: National Broadcasting Company.

Johnson, K. (1987, June 17). Goetz is cleared in subway attack; gun count upheld; acquittal won in shooting of four youths; prison term possible on weapon charge. *The New York Times*. Retrieved from http://www.nytimes.com/1987/06/17/nyregion/goets-cleared-subway-attack-gun-count-upheld-acquittal-won-shooting-4-youths.html

Johnston, L. (1996). What is vigilantism? *British Journal of Criminology*, 36(2), 220-236.

Lemon, S. (2008). Chinese police detain woman over quake video. *PC World*. Retrieved from http://www.pcworld.com/article/146171/article.html

Leyden, J. (2011). Anonymous shuts down hidden child abuse hub. Retrieved from http://www.theregister.co.uk/2011/10/24/anonymous_fight_child_abuse_network/

Library of Congress (2015). *S.754 - Cybersecurity Information Sharing Act of 2015*. Retrieved from https://www.congress.gov/bill/114th-congress/senate-bill/754

Liebowitz, M. (2011). Ip addresses of alleged child porn viewers released. Retrieved from http://www.nbcnews.com/id/45147364/ns/technology_and_science-security/

Marx, G. & Archer, D. (1976). The urban vigilante. *Psychology Today*, 7, 45-50.

Mentor, The. (1986). Hacker's manifesto. *Phrack Magazine*. Retrieved from http://phrack.org/issues/7/3.html

Merriam-Webster (2015). Vigilante. Retrieved from http://www.merriam-webster.com/dictionary/vigilante

Murphy, J. (2010). Shadows of doubt. Retrieved from http://www.sanjose.com/2010/09/08/09_08_2010_shadows_of_doubt/

Nojeim, G. & Butler, J. (2015, October 23). Guide to cybersecurity information sharing act amendments. Retrieved from https://cdt.org/blog/guide-to-cybersecurity-information-sharing-act-amendments/

Perverted Justice. (2008). Frequently asked questions. Retrieved from http://www.perverted-justice.com/index.php?pg=faq

Perverted Justice (2006). Celebrating the 100th conviction! Retrieved from http://www.perverted-justice.com/?updates=recent&offset=40

Rosenbaum, H. J. & Sedberg, P. C. (1976). *Vigilante Politics*. Pennsylvania: University of Pennsylvania Press.

Schultz, M. (2004, March 16). Online Vigilantes hunt down pedophiles. *USA Today*. Retrieved from http://usatoday30.usatoday.com/tech/news/internetprivacy/2004-03-16-online-vigilantes_x.htm

Skoric, M. M., Chua, J. P. E., Liew, M. A., Wong, K. H. & Yeo, P. J. (2010). Online shaming in the Asian context: Community empowerment or civic vigilantism? *Surveillance & Society*, 8(2), 181-191.

Stone, M. (2011). Anonymous exposes pedophile ring - hacks lolita city. Retrieved from http://www.examiner.com/article/anonymous-exposes-pedophile-ring-hacks-lolita-city

Sulzberger, A. G. (2010, December 15). Town mute for 30 years about bully's killing. *The New York Times.* Retrieved from http://www.nytimes.com/2010/12/16/us/16bully.html?_r=0

Tan, K. (2008). Online lynch mobs find second post-quake target; Liaoning girl detained by the police. *Shanghaiist*. Retrieved from http://shanghaiist.com/2008/05/22/online_lynch_mo.php

Tao, A. (2013). "I come from an influential family," says Honda driver who nicks 10-year old girl inciting near-riot. *Beijing Cream*. Retrieved from http://beijingcream.com/2013/05/i-come-from-an-influential-family-says-honda-driver/

Tor Project (2015). Tor: Overview. Retrieved from https://www.torproject.org

Tuovinen, L. & Röning, J. (2007). Baits and beatings: Vigilante justice in virtual communities. In *Proceedings of CEPE 2007. The 7th International Conference of Computer Ethics: Philosophical Enquiry* (pp. 397-405).

Wines, M. (2010). China's censors misfire in abuse-of-power case. *Herald-Tribune*. Retrieved from http://www.heraldtribune.com/article/20101118/ZNYT03/11183012

Xiao, F. (2010). Police Director's son kills girl in drunken hit run. *Epoch Times*. Retrieved from http://www.theepochtimes.com/n2/china-news/police-directors-son-kills-a-girl-while-driving-drunk-44699.html