Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

The hazards of cyber-vigilantism

Jeff Kosseff *

United States Naval Academy, Annapolis, MD, United States

Keywords:
Cybercrime
Vigilante
Social media
Hacking

A B S T R A C T

In recent years, some aggressive actions against cyber-criminals and terrorists have come not only from state actors, but also from independent third parties such as Anonymous. These groups have claimed some significant victories in their battles against ISIS and similar organizations, by hacking their email, publicly exposing their secret communications, and knocking their websites offline. The hacker groups also combat other cyber criminals, including distributors of child pornography. Some of the groups' activities, however, violate the computer hacking laws of many nations. Some commentators have criticized these statutes, claiming that the laws unnecessarily prohibit private actors from serving the public good.

In this Essay, I defend the broad prohibition of cyber-vigilantism, and argue that well-intentioned private actors can accomplish their goals by working with governments. I first review global jurisprudence, case studies, and academic commentary to explain why courts and policymakers historically have disfavoured vigilantism in other contexts, and I apply that reasoning to cyberspace. I explain that cyber-vigilantism can lead to several negative consequences, including the potential for abuse of the system, undercutting the legitimacy of democratic systems, and disproportionate punishments that are not necessarily effective. I then argue that instead of operating independently, these private groups can more effectively collaborate with governments and other private actors to fight threats in cyberspace.

1. Introduction

In November 2015, Isdarat, an ISIS propaganda website, was knocked offline and replaced with an advertisement for an online medication vendor. A message appeared above the advertisement, stating that "[t]oo many people are into this ISIS stuff," and urging visitors to "enhance your calm."[1]

What initially appeared to be a joke was actually a coordinated effort to disrupt ISIS's vast communications and propaganda network. Isdarat is one of hundreds of ISIS-affiliated websites to have been knocked offline by GhostSec and its affiliate, Anonymous.[2] These hacktivist groups have declared an online campaign against ISIS, and have vowed to disrupt its communications infrastructure.[3]

At first glance, such efforts appear to be in the public interest. After all, ISIS has mobilized a large network of supporters, in part because of its ability to communicate online and spread propaganda.[4] However, the means used by hacktivists often violate many nations' computer hacking laws, such as the

* United States Naval Academy, 121 Blake Road, Annapolis, MD 21402, USA.
E-mail address: kosseff@usna.edu.

[1] Jennifer Newton, *ISIS Website on the Dar Web is Hacked and Replaced with an Advert for Viagra and Prozac and a Message Telling its Supporters to 'Calm Down,'* Daily Mail (Nov. 25, 2015).

[2] Anthony Cuthbertson, *Hackers Replace Dark Web ISIS Propaganda Site with Advert for Prozac*, Int'l Bus. Times (Nov. 25, 2015).

[3] *See* Anthony Cuthbertson, *Anonymous #OpParis: Hacktivists Publish 'Noob's Guide' for Fighting Isis Online*, Int'l Bus. Times (Nov. 17, 2015).

[4] *See* J.M. Berger and Jonathon Morgon, The Brookings Project on U.S. Relations with the Islamic World, The ISIS Twitter Census: Defining and Describing the Population of ISIS Supporters on Twitter (March 2015).

http://dx.doi.org/10.1016/j.clsr.2016.05.008

Computer Fraud and Abuse Act[5] in the United States and the European Union member laws that implement the European Union Directive on Attacks Against Information Systems.[6] Although the scope of these laws varies, they generally prohibit unauthorized access or damage to computer systems and websites, and do not provide safe harbours for vigilantes.[7]

The efficacy of hacktivist groups has caused some to question whether nations should allow such hackers to fight ISIS – and other terrorist or criminal groups – by obtaining information from their computers or online services without authorization or causing damage to their computers or communications systems.[8]

As a practical and political matter, it is unlikely that members of GhostSec or Anonymous would be prosecuted under computer hacking statutes for disrupting ISIS's activities, as governments could exercise prosecutorial discretion and choose not to pursue individuals who seek to battle terrorist organizations.[9] However, cyber-vigilantism reaches far beyond battles against ISIS. In a variety of contexts, cyber-vigilantism has been a useful tool against hackers, terrorists, and online criminals. For instance, in 2011, Anonymous shut down one of the largest sources of online child pornography and posted personal details of more than 1500 of the host's users.[10] These cases – and the criticisms of computer hacking statutes – raise a broader question that policymakers around the world must address: should legal systems permit cyber-vigilantism? By exempting cyber-vigilantism from computer hacking laws, governments could be viewed as implicitly endorsing – and relying upon – cyber-vigilantes.

Highly skilled private groups – untethered from the many constraints and rules that bind governments – often can be more nimble in pursuing bad actors in cyberspace. For that reason, it is tempting to provide private hackers with broad leeway to battle terrorists, criminals, and other bad actors.

In this Essay, I explain why governments should resist this temptation. Courts and scholars long have cautioned against vigilantism, a term that I define in Part 2 of this Essay. As I explain in Part 3, the reasoning that has discouraged vigilantism in the physical realm applies equally in cyberspace. Although private hackers may be well-intentioned – and, in some cases, more skilled and effective than governments – it would be dangerous and short-sighted to delegate the roles of police, judge, jury, and punisher to private parties that exist outside of the democratic system. In Part 4, I propose an alternative, collaborative model in which private actors help governments to accomplish shared goals.

2. Defining cyber-vigilantism

At the outset, it is useful to define cyber-vigilantism for the purposes of this Essay, as the term carries many meanings.

For instance, some commentators argue that vigilantism only occurs when a group *illegally* uses *violence* to administer its conception of justice.[11] Such a definition is too narrow. To be sure, vigilantism includes illegal use of violence,[12] but it also encompasses other behaviour in which private actors seek to independently play the role of law enforcement. Particularly in the cyber realm, a number of activities – such as data theft or denial of service attacks – may not appear to be "violent" in the traditional, physical sense, but nonetheless involve private citizens taking the law into their own hands.

Moreover, whether an act is "vigilante" behaviour should not necessarily turn on the legality of the vigilante's actions. For instance, even if nations were to amend their hacking laws to allow the activities of Anonymous and GhostSec, those activities still should inherently be considered vigilantism, in that they involve private groups taking the law into their own hands.[13] The inquiry for the purposes of this Essay is whether states should allow private parties to engage in cyber-vigilantism without facing the penalties of law. Even if certain forms of hacking were legal, they still would be considered vigilante if they enable private parties to play the role of law enforcement.

[5] 18 U.S.C. § 1030.

[6] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems.

[7] Similarly, the Budapest Convention on Cybercrime, which requires signatories to establish criminal offenses for illegal access, interception, interference, and other computer crimes, does not contain a clear exception for vigilante behaviour. However, it permits nations to require a showing of "dishonest intent" or similar states of mind before criminal liability attaches for some of the acts. *See* ETS 185 – Convention on Cybercrime, 23.XI.2001.

[8] *See* Taylor Luck, *Have U.S. Laws Created an Online Haven for Islamic State Propaganda? Christian Science Monitor* (Aug. 25, 2015) (stating that that some analysts believe that the CFAA has led ISIS "to use US-hosted websites as its channel of choice to reach out to its followers"); Jessica Herrera-Flanigan, *Make Way for the Lone Cyber Ranger and Online Vigilantism*, Nextgov Cybersecurity Report (March 15, 2013) ("The potential for cyber vigilantism could be tremendous with limitations and safeguards in place."); Trevor A. Thompson, *Terrorizing the Technological Neighborhood Watch: The Alienation and Deterrence of the 'White Hats' Under the CFAA*, 36 Fla. State Univ. L. Rev. 537. 538 (2009) ("Current laws arguably reflect a near strict liability standard that stands at odds with traditional hacking principles such as exploration and innovation.").

[9] *See* Bjorn Carey, *Stanford Cybersecurity Expert Analyzes Anonymous' Hacking Attacks on ISIS*, Stanford Rep., http://news.stanford.edu/news/2015/november/lin-anonymous-isis-111815.html ("It's vigilante justice in cyberspace, which is illegal under the Computer Fraud and Abuse Act. On the other hand, while the U.S. government might not be favorably disposed to it, I think it is unlikely that any prosecutor would actually indict an American for harassing ISIS in this way.").

[10] Daniel Bates, *Hacker Group Anonymous Performs 'Vigilante' Attack on Online Child Porn Hub*, *Daily Mail* (Oct. 27, 2011).

[11] *See* Douglas Ivor Brandon, et al., *Self-Help: Extrajudicial Rights, Privileges and Remedies in Contemporary American Society*, 37 Vand. L. Rev. 845, 891 (1984) (defining vigilantism as "when citizens of a community band together and violently exercise police power authority in an unlawful manner, as abhorrent to the fair and predictable administration of justice.").

[12] *See, e.g.*, Azogu F. Adigwe, *Crime, Vigilantism, and Electoral Violence in Nigeria*, *Int'l J. of Human. and Soc. Sci. Invention* 46 (2013).

[13] *See* Les Johnson, *What is Vigilantism? Brit. J. of Criminology* 220–226 (1996) ("For even where self-help groups enjoy a potential to exercise or threaten force that potential may not, it itself, be unlawful. Illegal and extra-legal action are not, therefore, preconditions of vigilantism.").