Ethics of Hacktivism

MAJ Tennille W. Scott, M.S., University of Maryland University College
Student

O. Shawn Cupp, Ph.D., Kansas State University
Professor

US Army Command and General Staff College
ATTN: Department of Logistics and Resource Operations (DLRO)
Room 2173B
100 Stimson Avenue
Fort Leavenworth, KS 66027
Voice: 913.684.2983
Fax: 913.684.2927

tennille.w.scott.mil@mail.mil
orville.s.cupp.civ@mail.mil

Authors' Financial Disclosure – I have no conflict of interest, including direct or indirect financial interest that is included in the materials contained or related to the subject matter of this manuscript.

Disclaimer:

Introduction

Do hacktivists have ethics? Some would say yes and others would suggest that no, they do not. Are there rules that those who engage in hacking follow or abide by during the conduct of their activities? Does the hacktivist maintain any semblance of actions that can be described under the Just War theory? If so, it would seem to be only in Jus in Bello[1] or the just conduct in war, due to the perpetual nature of hacker activities and hacktivist operations. But that may be the subject of another paper.

First, what is a hacktivist?[2] They can be defined as those who through the nonviolent use for political ends of "illegal or legally ambiguous digital tools" like website defacements, information theft, website parodies, denial-of-service attacks, virtual sit-ins, and virtual sabotage.[3] This provides the basis for understanding more about where hacktivists' motivations come from and what kinds of ideologies they may exhibit.

Nevertheless, hacktivists must conform to some sort of norm, right? Based upon the nature of hacktivist activities there must be a way to categorize or identify their overarching ethic. Understanding the motivation of this group is a huge undertaking because of the great variance and diversity of the people who make up the hacktivist collective. Unlike cyberterrorists, who typically belong to a hierarchical group structure and have a common cause, hacktivists are not bound in the same way, which makes them more dynamic and difficult to analyze. A prime example is the hacktivist group known as Anonymous and its spinoff group,

[1] Brian Orend, The Morality of War, Orchard Park, New York, 2006, 105.
[2] Alexandra Whitnbey Samuel, Hacktivism and the Future of Political Participation, (Sept 2004) (unpublished Ph.D. dissertation, Harvard University), available at http://www.alexandrasamuel.com/dissertation/pdfs/Samuel-Hacktivism-entire.pdf.
[3] Noah C.N. Hampson, Hacktivism: A New Breed of Protest in a Networked World, Boston College International and Comparative Law Review, Vol 35, Issue 2, 2012, p. 514.

Lulz Security (LulzSec), who would eventually participate in different activities with different motives.

The future of cyber warfare will include hacktivists, either as full combatants or as proxies, and understanding the underlying ethics of their activities provides context for decision-making throughout all levels of war. Understanding the ethical construct of hacktivists will assist in leveraging those areas within cyberspace that we can manage or in small segments dominate for short periods. The ethical construct of hacktivism will also allow us a better overall sense of "how things are done" within cyberspace, which translates directly into securing vital national security interests across the globe.

Problem Statement

Somewhere in the history of hacktivists and their interaction with cyberspace one would suggest that rules do exist for their conduct. However, understanding the motivations of hacktivists would provide the context to answer the ethical question. These rules may not rely or be built upon the traditional set of values we understand that are associated with fully developed theoretical models of ethical behavior. Although some commonalities exist within the self-justification of the activities of hacktivist groups, it is impossible to bound them to a common ruleset regarding ethical decision-making.

Thesis statement: Current ethics frameworks are not sufficient for classifying hacktivists, their actions, or motives. We propose models consisting of an asymmetric view and application of a complexity framework to analyze hacktivism in today's environment. These models provide context and predictability to better understand the impact of hacktivist ethics on the future of warfare.

Social contract theory answers the question of the reason to act moral – because "people collectively agree to behave morally as a way to reduce social chaos and create peace."[4] In this case, most hacktivist are probably not wanting to reduce social chaos but increase it. This is evident considering "the lifeblood of the hacker ethic has always been the freedom of information and the full democratization of the public sphere."[5]

Many others have described a "hacker ethic." Steve Levy described two maxims in his book *Hackers* in 1984. They are "all information should be free and mistrust authority and promote decentralization."[6] This seems to be really three maxims but for arguments sake we will treat them as two. This freedom of information pledge is evident in a number of theorists and writers who state that all information should be available to everyone in society. This is the ultimate in execution of Levy's twin maxims of hacker ethic.

Categorization of Hacktivists

The term hacktivist is used to describe a person who conducts computer hacking in order to promote an activist agenda, but there are people within hacktivist groups and who participate in hacktivist activities who neither have no hacking skills nor actually hack systems. Often, the lines between activism, hacktivism, and cyberterrorism are blurred and hacktivist activity is misidentified.[7] The definition for hacktivist should be broadened to represent one who leverages technology to promote social activism.

[4] Lois P. Pojman and James Fieser, Ethics Discovering Right and Wrong, Boston, Massachusetts, 2012, 65.
[5] Mark Manion and Abby Boodrum, Terrorism or Civil Disobedience, Computers and Society, June 2000, 18.
[6] Peter Ludlow, Wikileaks and Hacktivist Culture, The Nation, October 4, 2010, 25.
[7] John Arquilla and David Ronfeldt, Networks and Netwars: The Future of Terror, Crime, and Militancy, available at http://www.rand.org/pubs/monograph_reports/MR1382.html, 2001, 241.

Hacktivist attacks were by previously categorized by identifiable individuals or groups and their motivations. In the past, White Hats, Black Hats, and Gray Hats were hackers and activists motivated by a particular means or agenda. Their motivations were usually placed upon a linear scale or continuum with White being good, Black being bad, and Gray somewhere in-between. Now, hacktivists consist of a number of subgroups with a variety of motivations that cannot be secured to a good-bad continuum. The scaled metric no longer applies because the positions of individuals and groups do not fit neatly into clearly defined categories. They appear more on a circular basis with a variety of motivations and positions.

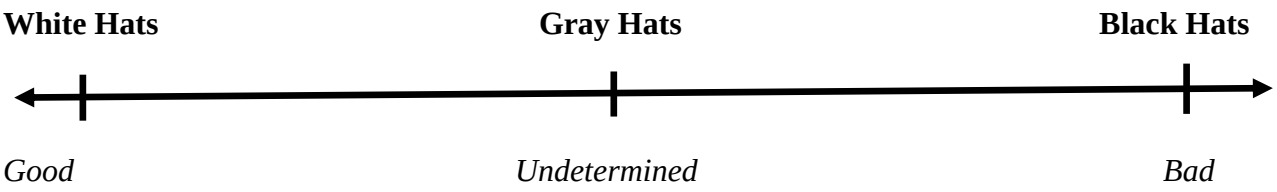

Figure 1.1 Conventional Thinking of Hacktivists and their motivations

Red Hats, Green Hats, Yellow Hats, Orange Hats, Purple Hats, and Blue Hats are possibilities for different categories of hacktivists. These categories could be based upon religion, global region, political ideology, social status, economic considerations, etc. The fundamental realization is that all hacktivists can no longer be categorized on a continuum (see Figure 1.1). Their positions are far too diverse and their motivations are even more varied. Purposes are no longer singular and linear, but are across a variety of positions. These positions could be categorized in a variety of colored hats to keep with the current typology. Figure 1.2 shows one way to portray these various groups or individuals. Not only are motivations different but they are also based upon the characteristics of using cyberspace to further a group's agenda.

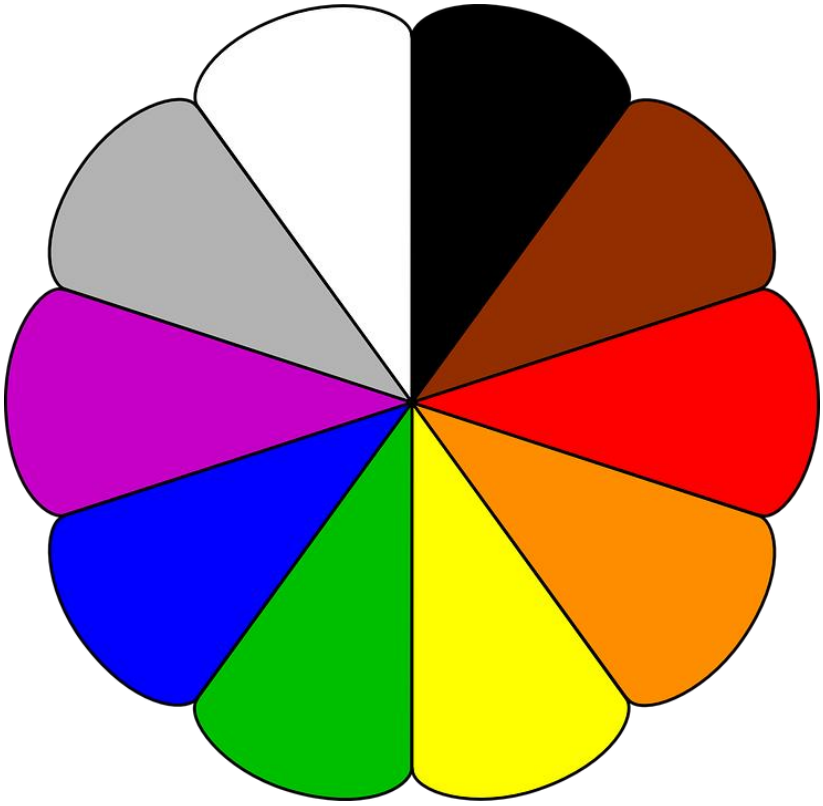

Figure 1.2 Proposed circular positions and motivations of hacktivists

Characteristics of Cyberspace

Understanding the ethics of hacktivists requires that we understand the operating environment where they operate. Defining cyber is a difficult task as shown by the slow adaptation by the U.S. government of developments in cyber.[8] There exists a need to develop and debate a comprehensive theory of cyberspace. Up until this date, parts of this military domain were debated and discussed; however, a single holistic theory eludes contemporary theorists. Table 1.1 compares military domains and current characteristics of those domains in

[8] Megan L. Ortagus, The Internet's Impacts on Power Differentials in Security and Conflict, Baltimore, Maryland, 2014, 14.

terms of military use. These comparisons provide the basis to determine if new principles of warfare are required for the cyberspace domain.

The major cyberspace characteristics that hacktivists rely on are accessibility, internetworking, and sociability. The absence of these three elements makes it difficult for hacktivist groups to achieve their agenda. Accessibility is the core of the hacker subculture and the attribute largely at odds with the law. Anyone can acquire equal access to cyberspace. Internetworks provides a means to share data and information globally. Sociability gives individuals the convenience of socializing in the virtual space and allows them to expand their influence in a way that would be otherwise difficult or impossible. Cyberspace affords hacktivists an optimal platform for planning, organizing, and executing their activities.

Principles of Cyberspace

Below are some central principles of cyberspace derived from the comparison above and a review of the current literature. These primarily describe cyberspace but do have connections to the other domains of military conflict. "Cyberspace differs fundamentally from the traditional physical domains. It requires as much of a reexamination of basic principles as did air, relative to land and sea warfare."[9] It is the domain of warfare based upon connectivity,[10] and may require different principles of warfare.[11]

*Continuous of the domain—C*yberspace is ever expanding and constantly adding to the domain, almost infinite in propensity. It is the only domain of warfare that is in a constant state

[9] Sean C. Butler, Major Refocusing Cyber Warfare Thought, *Air and Space Power Journal*, Jan-Feb, 2013, 54.
[10] Thomas M. Chen, "An Assessment of the Department of Defense Strategy for Operating in Cyberspace," The Letort Papers, Strategic Studies Institute, U.S. Army War College, Carlisle, PA, 2013, 6.
[11] Raymond C. Parks, and David P. Duggan, Proceedings of the 2001 IEEE, Workshop on Information Assurance and Security, United States Military Academy, West Point, NY, 2001, 122.

of replicating itself.[12] It is not constrained by borders or boundaries. Cyberspace is endlessly increasing in size, scale, and scope.

Domain	Physical	Virtual	Cognitive	Connect with other Domains	Dominance can be exerted over Domain	Nation State Sponsored Requirement	Non-State Actor Usage	Growing as a Domain
Land	*Yes*	*No*	*No*	*Yes*	*Yes*	*Yes*	*Yes*	*No*
Sea	*Yes*	*No*	*No*	*Yes*	*Yes*	*Yes*	*Maybe*	*No*
Air	*Yes*	*No*	*No*	*Yes*	*Yes*	*Yes*	*Manned Unlikely*	*No*
Space	*Yes*	*No*	*No*	*Maybe*	*Maybe*	*Yes*	*Unlikely*	*Maybe*
Cyber	*Yes*	*Yes*	*Yes*	*Yes*	*No*	*No*	*Yes*	*Yes/infinite*

Table 1.1 Comparison of Domains

Flattening of operational environment—strategic, operational, and tactical levels of war are no longer adequately descriptive of the cyberspace domain. They are flattened into a single "plane" or level of war. "Achieving global cyber superiority or global cyber control by any organization is no longer technically possible."[13] Cyberspace is no longer an area that is divided into level of war nor is it a domain that an entity (nation state, non-state, nor criminal actor) can exhibit dominance over.

Physical destruction not necessary—It is the domain in which a nation state or a non-nation state actor can attack, destroy, degrade, or affect an enemy without causing physical destruction.[14] Historically, the preponderance of attacks through the land, sea, air, and space

[12] John B. Sheldon, Deciphering Cyberpower Strategic Purpose in Peace and War, *Strategic Studies Quarterly*, Summer, 2011, 95-112.
[13] Martin R. Stytz and Shela B. Banks, Toward Attaining Cyber Dominance, *Strategic Studies Quarterly*, Spring 2014, p. 55.
[14] Phillip S. Meilinger, The Mutable Nature of War, *Air & Space Power Journal*, Winter, 2010.

must include physical destruction to influence an enemy. Nonlethal effects can be achieved persistently through cyberspace.

Multi-symmetrical—As opposed to other military actions namely symmetric and asymmetric warfare, cyberspace is multi-dimensional in nature and in use of this domain by state, non-state, and criminal actors. Cyberspace is greater than the sum of its technological parts.[15] Access to other domains is instantaneous and cyberspace is the only military domain that can influence all the other domains of warfare. In fact, it is the only domain where one can operate and influence all the other domains.

Politics is not required— Fundamentally, cyberspace can also no longer be adequately described by Clausewitz definition of warfare as merely an extension of politics.[16] There may be no political purpose or goal to their attacks but "cyberspace will be an integral part of future warfare."[17] Some may say that this will end in politics of chaos. That may be true, but with the Internet we have a new series of entities to deal, manage, or mitigate, which includes the "hacktivist."

Defense Industrial Base not required— During World War I, capital ships were measured as a national expenditure and defined as such, however this rubric is no longer valid in cyberspace. As for today, large industrial manufacturing plants, both mechanical and electronic, are not required for one to engage or even dominate within this domain.

Given the principles above, one can clearly see the ease at which a noncombatant, such as a hacktivist, could participate in cyberwarfare.

---

[15] Hans-Inge Langø, "Slaying Cyber Dragons: Competing Academic Approaches to Cyber Security," NUPI Working Paper 820, Norwegian Institute of International Affairs, Oslo, Norway, 2013, 27.
[16] Thomas Rid, Cyber War Will Not Take Place. *Journal of Strategic Studies*, 35, 2012, No. 1, 5-32.
[17] Thomas Chen, An Assessment of the Department of Defense Strategy for Operating in Cyberspace, The Letort Papers, Carlisle, PA., 2013, 10.

A Proposal for Understanding Hacktivism Ethics

Usually when a practicing or overarching ethic is identified it is for a group. There are group norms and rules that govern the operations and activities of that group. One prominent group in hacktivist circles is Anonymous. Anonymous is "everything and nothing," have "no structure or leader," and reveal themselves "more like *Fight Club* due to the rules that they do reveal to the public."[18] But, besides these obscure operating instructions, there should be some kind of definitive rule set that could be applied, understood, and used.

Our current understanding of hacker ethics expands on Levy's description and are emphasized in the Hacker Manifesto written by The Mentor and the Guerilla Open Access Manifesto written by Aaron Swartz. Today, the principles of freedom of access to information, freedom of information sharing, and freedom to explore intellectual curiosity are only a fraction of the motivations within the hacktivist culture. The color wheel model provides a one-dimensional understanding of hacker motivations, but the Cynefin framework proffers a means to analyze the complexity of hacktivist culture in its entirety.

The Cynefin framework (Figure 1.3) was developed to help leaders visualize and understand interactions of systems within various environmental conditions. The purpose is to give decision-makers the ability to analyze where their systems lie in order to affect outcomes. The external environment is represented by a continuum of ordered and unordered states and within this continuum are five domains in which systems operate: Simple; Complicated; Complex; Chaotic; and Disorder.[19] These domains represent various levels of knowledge and

[18] Parmy Olsen, We Are Anonymous: Inside the Hacker World of LulzSec, Anonymous, and the Global Cyber Insurgency, New York, New York, 2012, 7.
[19] William Dettmer, Systems Thinking and the Cynefin Framework: A Strategic Approach to Managing Complex Systems, http://www.goalsys.com/books/documents/Systems-Thinking-and-the-Cynefin-Framework-Final.3.pdf, 2011, 10.

available information about a system. This framework is advantageous for military leaders because they constantly operate in dynamic environments which often require solutions to problems of varying complexity.

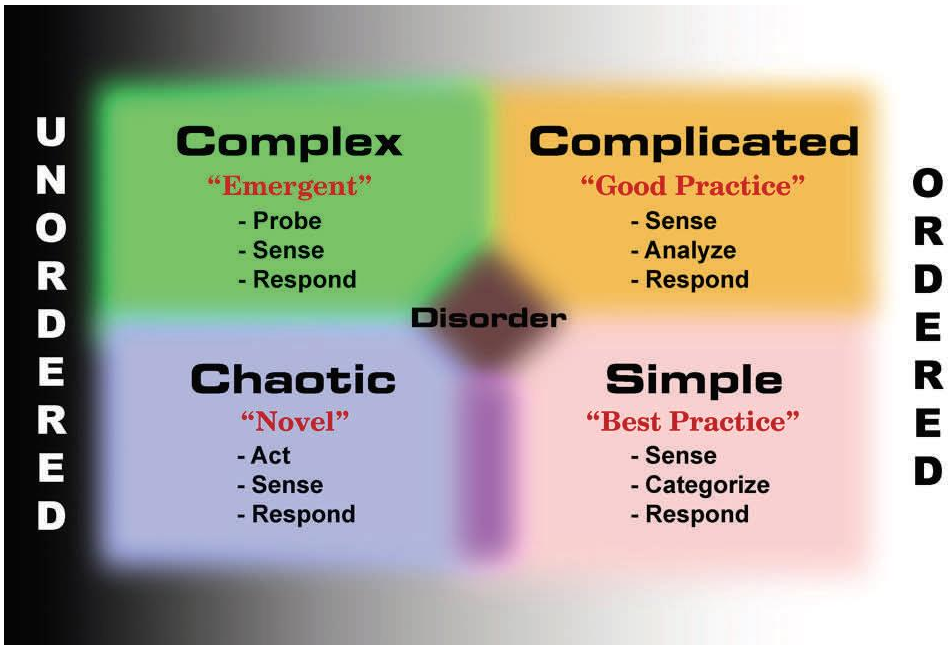

Table 1.2 The Cynefin Framework. Retrieved from Goal Systems International, "Systems Thinking and the Cynefin Framework," accessed March 17, 2017, http://www.goalsys.com/books/documents/Systems-Thinking-and-the-Cynefin-Framework-Final.3.pdf

The ethical construct of hacktivism can be aligned with the simple, complicated, complex and chaotic domains of the Cynefin framework, which also represents varying levels of context and predictability. For example, Anonymous' campaign against the Church of Scientology in 2008, also known as Project Chanology, morphed from a simple problem of pranks to a complex problem of global street protests, in a few weeks' time. The members of Anonymous went from being labeled as computer geeks to cyberterrorists and everything between, even though there are Anonymous members who are not hackers. Technology is now leveraged for activism in a way

that makes it impossible to categorize these activities linearly because regular computer users are also able to participate in hacktivist efforts in legitimate ways.

Table 1.3 shows the Cynefin framework applied to two different instances of hacktivism: Anonymous hacktivist group and Edward Snowden. Anonymous activity spanned across three domains, from simple to complex, representing behaviors and motives that range from explainable connections to unexplainable connections. Edward Snowden's case represents the chaotic domain where connections are not obvious or explainable, and therefore not predictable, but may reveal connections after subsequent analysis.

Complex Domain (Unknown knowns)	**Complicated Domain** (Known Unknowns)
Actor: Anonymous **Motivation:** Expose rights violations **Target:** Church of Scientology **Method:** Street protests (global)	**Actor:** Anonymous **Motivation:** Protest Internet censorship **Target:** Church of Scientology **Method:** Denial of Service, Google bomb
Chaotic Domain (Unknown unknowns)	**Simple Domain** (Known knowns)
Actor: Edward Snowden **Motivation:** Whistleblowing **Target:** National Security Agency **Method:** Retrieved classified documents	**Actor:** Anonymous **Motivation:** "Lulz" (laughs) **Target:** Church of Scientology **Method:** Pranks (phone calls, emails, faxes)

Table 1.3 Application of the Cynefin Framework

Conclusion

Framing the operational environment in the cyber domain will be a critical step for conducting multi-domain operations in the future. The characteristics and principles of cyberspace affords hacktivists an optimal platform for planning, organizing, and executing their activities. Linear categorization of hacktivist activity is no longer sufficient to understand their motives. Hacktivists cannot be ignored in future warfare because the evolution of their activity suggests increasing complexity of actors, motivations and targets. The Cynefin framework provides a means for military leaders to understand the ethical decision-making of hacktivists and the impact of their actions on future warfare. Understanding the ethical construct of hacktivists will assist in leveraging those areas within cyberspace that we can manage or dominate for short periods. We can also gain a different perspective of operating within cyberspace, which translates directly into securing vital national security interests across the globe.

Bibliography

Arquilla, John and Ronfeldt, David, (2001). Networks and Netwars: The Future of Terror, Crime, and Militancy, available at http://www.rand.org/pubs/monograph_reports/MR1382.html.

Butler, Sean C., (2013) Major Refocusing Cyber Warfare Thought, Air and Space Power Journal, Jan-Feb.

Chen, Thomas M., (2013) An Assessment of the Department of Defense Strategy for Operating in Cyberspace, The Letort Papers, Strategic Studies Institute, U.S. Army War College, Carlisle, PA.

Dettmer, William, (2011). Systems Thinking and the Cynefin Framework: A Strategic Approach to Managing Complex Systems, available at http://www.goalsys.com/books/documents/Systems-Thinking-and-the-Cynefin-Framework-Final.3.pdf.

Hampson, Noah C.N., (2012). Hacktivism: A New Breed of Protest in a Networked World, Boston College International and Comparative Law Review, Vol 35, Issue 2.

Langø, Hans-Inge, (2013). Slaying Cyber Dragons: Competing Academic Approaches to Cyber Security, NUPI Working Paper 820, Norwegian Institute of International Affairs, Oslo, Norway.

Ludlow, Peter, (2010). Wikileaks and Hacktivist Culture, The Nation, October 4.

Manion, Mark and Boodrum, Abby, (2000). Terrorism or Civil Disobedience, Computers and Society, June.

Meilinger, Phillip S., (2010). The Mutable Nature of War, *Air & Space Power Journal*, Winter.

Olsen, Parmy, (2012). We Are Anonymous: Inside the Hacker World of LulzSec, Anonymous, and the Global Cyber Insurgency, New York, New York.

Orend, Brian, (2006). The Morality of War, Orchard Park, New York.

Ortagus, Megan L., (2014) The Internet's Impacts on Power Differentials in Security and Conflict, Baltimore, Maryland.

Parks, Raymond C. and Duggan, David P. Duggan, (2001). Proceedings of the 2001 IEEE, Workshop on Information Assurance and Security, United States Military Academy, West Point, NY.

Pojman, Lois P. and Fieser, James, (2012). Ethics Discovering Right and Wrong, Boston, Massachusetts.

Rid, Thomas, (2012). Cyber War Will Not Take Place. Journal of Strategic Studies, 35, No. 1.

Samuel, Alexandra Whitnbey, (2004). Hacktivism and the Future of Political Participation, (unpublished Ph.D. dissertation, Harvard University), available at http://www.alexandrasamuel.com/dissertation/pdfs/Samuel-Hacktivism-entire.pdf.

Sheldon, John B., (2011). Deciphering Cyberpower Strategic Purpose in Peace and War, Strategic Studies Quarterly, Summer, 2011.

Stytz, Martin R. and Banks, Shela B., (2014). Toward Attaining Cyber Dominance, Strategic Studies Quarterly, Spring.