AU/ACSC/LIDOWSKI, R/AY15

AIR COMMAND AND STAFF COLLEGE

AIR UNIVERSITY

ANONYMOUS AS A CYBER TRIBE: A NEW MODEL FOR COMPLEX, NON-STATE CYBER ACTORS

by

Robert L. Lidowski, Major, USAF
MS, Computer Science

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements for the Degree of

MASTER OF OPERATIONAL ARTS AND SCIENCES

Advisor: Dr. Angelle A. Khachadoorian

Maxwell Air Force Base, Alabama

May 2015

Disclaimer

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Abstract

The online collective Anonymous is a complex cyber actor that exhibits many elements of a tribal culture. It represents a new class of cyber actor that, like tribal societies, derives meaning from place, follows an influence-based leadership model, and conducts war for reasons not readily understood by modern nation-states. Anonymous challenges the usefulness of contemporary military doctrine. A comparison between Anonymous' cultural features and those of non-cyber tribes shows how military strategists can apply the "cyber tribe" concept as a starting point for understanding complex, non-state cyber actors. The US military should update doctrine to recognize the role of place, values/norms, community sustainment mechanisms, and motivations in planning operations that affect cyber tribes and their indigenous cyber-personas. Only then can cyber strategists exercise the required amount of cultural relativism needed to influence complex, and sometimes disturbing, non-state cyber actors.

Contents

Introduction

The current conflict with the Islamic State (ISIS) highlights the US military's challenges in cyberspace. In a sense, ISIS represents the most recent entry in a list of adversaries that the US has treated as monolithic, only to discover a far more complex network of actors. The US experienced this learning curve with Al Qaida, Afghan tribal groups in Operation Enduring Freedom, and an Iraqi insurgency in Operations Iraqi Freedom and New Dawn. The online collective Anonymous represents a similarly complex actor in cyberspace that remains unexamined in US joint doctrine. Further, Anonymous recently made itself more relevant to military operations by declaring its own parallel war on ISIS.[1] This parallel conflict complicates coalition military operations. Any potential intelligence gathering or operations conducted by the US against ISIS through cyberspace could conflict with Anonymous' methods, tools, results, or strategic goals. Understanding Anonymous, and cyber actors like it, requires a new model for analyzing non-state cyber actors. The US should examine non-state, transnational cyber actors using a tribal lens—that is, treat them as a tribe existing within cyberspace. A comparison between Anonymous' cultural features and those of non-cyber tribes demonstrates how a non-state cyber actor can operate as a "cyber tribe" and how military doctrine should be updated accordingly.

Background on Anonymous

Dr. Gabriella Coleman entitled her book on Anonymous *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous*. For two years she spent at least five hours a day observing Anonymous' conversations and operations.[2] Dr. Coleman immersed herself in a way that almost designated her as an honorary Anon (member of Anonymous). Despite her deep evaluation, the book's title still points to the universal difficultly of classifying the group's role in society. The

media sometimes identifies Anonymous as a "hacker collective,"[3] but this is inaccurate. Anonymous contains hackers and a great many technically-oriented non-hackers, but also non-technical contributors to the group's pranks or political protests.[4] Anonymous originated as early as 2004 on the /b/ message board of the photo-sharing website 4chan.org.[5] The group's original activities revolved around coordinated pranks designed to embarrass, enrage, or confuse the target. This evolved to include various forms of political protest and vigilante justice, but employed many of the same prankster tactics.[6] During highly publicized raids, Anonymous faced off against the Church of Scientology, the Motion Picture Association of America,[7] MasterCard, PayPal, US Senators,[8] and several foreign governments. It also put both a British law firm and a US security contractor out of business. Anonymous now comprises many splinter groups that share some basic norms and values, but differ widely in other respects. A few of the more famous sub-groups include Chanology, LulzSec, and AntiSec. This trend toward new splinter groups suggests a growing complexity that defies current doctrinal concepts for cyber actors.

While Anonymous employs a wide range of technology to accomplish its raids, this paper concerns itself with the small subset required to discuss human-to-human interaction in cyberspace. The important concepts that still require introduction are Internet Relay Chat, chat logs, and Internet Protocol addresses. Internet Relay Chat, or IRC, is a system for exchanging typed messages pseudonymously. Typically, an IRC user will create or join a "channel" to engage in group discussions. Anyone joining an active channel will see a list of other channel users as well as a scrolling display of text-based conversation. Chatting usually occurs in this group setting, but users can privately message each other. IRC facilitates large numbers of users chatting or listening simultaneously. Anonymous has created/used numerous IRC services to coordinate its operations, including AnonOps and Partyvan. Chat logs are records of previous

IRC chats that individuals may save for social reasons. Conversely, law enforcement may collect logs as criminal evidence. An Internet Protocol (IP) address is a series of numbers which specify where information should be delivered on the Internet. Discovering someone's IP address provides a target of attack or investigation. Cyber actors like Anonymous disguise their IP addresses to maintain anonymity. Both IP addresses and chat logs constitute traces of individual human activity within cyberspace.

Cyber Doctrine, Cyber-personas, and the Cyber Tribe

US military doctrine on cyberspace proves inadequate in its treatment of groups like Anonymous by underemphasizing the role of human interaction and culture in cyberspace. The unclassified portion of Air Force cyber doctrine recognizes the physical and logical elements of cyberspace, but excludes human interaction.[9] Joint cyberspace doctrine extends this model to include three layers: physical network, logical network, and cyber-persona.[10] A cyber-persona is a "digital representation of an individual or entity identity in cyberspace."[11] Joint Publication 3-12 provides this definition, but neglects to expand the concept enough to successfully guide operations.[12] Implementing a cyber-persona concept is certainly a step forward from Air Force doctrine. The cyber-persona concept, however, ignores the complexity of social interactions within cyberspace, which can give rise to group identities, political structures, social norms, values, decision making processes, and leaders. The cyber tribe model extends the concept of a cyber-persona to frame complex social interactions within cyberspace.

Cyber tribes, to modify Brian Ferguson's definition of tribes, are indigenous cyber-personas "outside the direct administration of a centralized, authoritative state."[13] Certainly, there are many groups that operate outside the bounds of state authority—terrorist networks, organized crime syndicates, and non-cyber tribal groups to name few. While these groups may maintain

cyber-personas, they only act *through* cyberspace. They use cyberspace, but also exist independently. Cyber tribes, by contrast, are indigenous, meaning group identity and individual cyber-personas are formed *within* cyberspace. If cyberspace ceased to exist tomorrow, cyber tribes would disappear whereas groups like Al Qaida would continue to exist. Since cyberspace operates outside the direct administration of any one nation state, these indigenous cyber-personas are free to form their own political structures and culture. Starting with a tribal concept of place, Anonymous provides a striking example of how closely these groups can resemble traditional tribal societies.

Anonymous as a Cyber Tribe

Like non-cyber tribes, Anonymous maintains and derives meaning from a sense of place. The concept of place is distinct from the concept of space and plays an important role in understanding tribal cultures. Space consists of meaningless physical features such as elevation and terrain. People socially construct place when they apply meaning, values, and stories to a space.[14] Space, as a philosophical and scientific concept, grew as the predominant Western worldview from the Renaissance through today.[15] It is therefore difficult for Western thinkers to shake this long-standing cultural norm and shift perspectives from space to place. The term "cyberspace" itself hints at the bias of Western culture. Yet place remains the dominant perspective among tribal cultures, and, for that reason, provides a promising start for establishing a cyber tribe model.

For tribal societies like the Yanyuwa of northern Australia, for example, the sense of place drives their "way of knowing the world" and cannot be separated from their culture.[16] The Internet bulletin board 4chan acts as Anonymous' tribal homeland and, therefore, shapes Anonymous' culture and structure. Instead of system administrators or software enforcing most

rules for posting on 4chan, the site's openness gave rise to a collectively-decided set of rules. Thus, human social interactions decided the meaning of 4chan instead of an inherent technical terrain, turning a portion of cyberspace into a "cyber place." 4chan users' collective decision to socially enforce anonymity on the site gave rise to Anonymous' name[17] as well as its cultural taboo against revealing non-cyber identities.[18] 4chan's egalitarian ethos provided a feeling of acceptance to its members,[19] engendering a sense of belonging and shaping a distinct lifestyle for a dedicated minority.[20] Like the Yanyuwa relationship to their homeland, Anonymous and its culture cannot be properly understood apart from its history on 4chan. The specific example of Anonymous and 4chan requires some theoretical broadening before we can replace space with place as an analytical lens for studying cyber tribes.

Reflecting on existing models of place and self provide the first step toward establishing cyber place and deepening the concept of cyber-persona. Writing from the nexus of philosophy, geography, and anthropology, Dr. Edward Casey provides a useful contemporary model for place. According to Dr. Casey, self and place exist in "constitutive coingredience: each is essential to the being of the other."[21] He proposes the terms "habitus," "habitude," and "habitation" as the mediating concepts between self and place. A habitude is a mental habit that results in recurring, concrete action within a given place. Habitus is the self's collection of ever-changing habitudes and thus serves as "the basis for action in… any given place."[22] The self enacts habitus by inhabiting place. In theoretical terms, habitation requires the self to be in a place by sensing place, holding place in memory, and absorbing place's ambiance. Enacting a habitude in a place alters the experience of others as they inhabit the same place, while habitation shapes the self's own habitudes.[23] In other words, habitus and habitation continually create and shape each other. Furthermore, habitus and habitation provide a measure of a place's strength, or

"habitudinal density." A place's habitudinal density is thick when the shaping force between habitus and habitation is strong. Habitudinal density is thin when the shaping force is weak.

Casey's philosophical model describes humans inhabiting physical places, but habitus and habitation apply equally well to cyber-personas inhabiting cyber places. Journalist Parmy Olson's interviews with various Anons reveal that participation in cyber places can become a way of life.[24] This inhabitation of cyber places creates habitudes particular to place. A cyber-persona inhabiting 4chan, for example, will only post content anonymously, but the same persona chatting on the Partyvan IRC system may operate pseudonymously under a consistent nickname. Violating either norm invites criticism from other Anons, which shapes the violator's habitudes. The magnitude of adoption of these habitudes by cyber-personas reveals the habitudinal density of any given cyber place. Casey dismisses interactions with electronic media as distractions that attenuate place, but also claims that this attenuation leads people to seek thick places.[25] Olson's interviewed Anons, however, experienced a thinning of physical places, which drove them to seek thicker experiences in cyber places like 4chan.

Anthropologist Gerald Gold found the same drive toward cyber place among on-line disability support communities. In Gold's research, multiple sclerosis attenuated community members' meaningful inhabitation of physical places. His "MSC-L" support group members developed distinctive reputations and created self-governance mechanisms within their cyber forum. MSC-L produced at least one self-identified influence leader that used "philosophical expressions to indicate to others whether he finds a thread to be a valuable insight or an inappropriate behavior." Interestingly, MSC-L's social interactions also evolved into limited forms of political protest.[26] Like Anons on 4chan, the support group developed its own norms

for appropriate behavior, which translated to cyber-persona actions—another illustration of place shaping habitudes.

By establishing cyber place, the cyber tribe model also establishes the tools and language required to theoretically expand the concept of cyber-persona. The cyber-persona found in joint doctrine is a rather thin concept that seems to represent nothing more than an organizational unit for reasonably assigning cyber activity to appropriate cyber actors. JP 3-12 notes that "cyber-personas can be complex, with elements in many virtual locations, but normally not linked to a single physical location or form."[27] This disjointed model of a cyber-persona reflects a space-biased view of the world that sees the persona's constituent parts while remaining blind to the integrative whole.

Shifting to a place-centric perspective, cyber-persona represents an extension of self that inhabits various cyber places. The persona's inhabitation forms and enacts habitudes which, in turn, shape the ambiance and memory of cyber place for other cyber-personas inhabiting the same place. Thus, a cyber operation could focus on affecting the cyber places a persona inhabits by inhabiting the same place. Alternatively, operations could strive to separate a relevant persona from its influential cyber places. Anonymous intuitively reflects a place view when it enforces its cultural norms, most notably when it banishes members from influential IRC channels and servers.[28] From a space-over-place perspective, the banished persona may only need to log back in under a new username. From a cyber place perspective, however, operating under a new username "means losing the stable marker of identity and reputation."[29] A cyber-persona's effective operation, therefore, depends on its habitation and good standing within cyber place.

Cyber-persona also represents wholeness through tribal reflections on personhood, synecdoche, and fractured self. "Personhood" encompasses a group's cultural concepts for

determining "what is a person." Synecdoche represents a common theme in tribal concepts of personhood wherein "parts of the body… and bodily secretions… retain lifelong influence" over the originator.[30] Leaving these parts and secretions unprotected opens one to curses and magical attacks. As Anons traverse the cyber world, they may leave behind identifying technical traces such as IP addresses and chat logs. These technical traces are akin to bodily traces of real world tribes in that leaving them unprotected opens Anons to attack and law enforcement activities. The prominent Anonymous hacker Sabu left screenshots of his exploits unguarded, which ultimately led law enforcement to an undisguised IP address and his real world identity. Sabu, in turn, provided chat logs and other technical trace material, which the FBI used to prosecute other Anons.[31]

While cyber-persona presents an integrated whole within the context of cyber places, a tribal model does not imply that a cyber-persona is fully integrated into its associated real-world persona. In other words, the "self" presented socially in the physical world may differ significantly from the "self" presented by a cyber-persona. The African Tswana tribe conceives of personhood as including the "sum total of… relations, presences, enterprises" over both space and time—a form of synecdoche. The Tswana fracture the self into context-specific facets which limits others' access to the parts and pieces needed for magical attack. For example, a Tswana tribe member may have a work-facet only shown to coworkers and a separate religious-facet only shown to fellow worshippers.[32] Similarly, the Anonymous hacker Kayla acted out the cyber-persona of a 16-year old girl complete with numerous back story details. In the physical world, "Kayla" was a British man in his twenties, but that truth mattered little to Kayla's fellow Anons who valued the cyber-persona as presented.[33] Like the Tswana, Kayla represented a fractured self meant only for an Anonymous-specific context. The differences between Western

mainstream culture and Anonymous' culture present the possibility that cyber-persona may be considered a fractured self within the cyber context.

The relationship between cyber place and cyber-persona offers important implications for understanding an adversary's point of view. Relevant non-state cyber actors may hold a place-centric view of the cyber world. Contrary to popular belief, Anonymous is not a hacker collective. Many active members contribute non-hacker skills and would not view their experience as "cyberspace." That is, relevant actors may experience their cyber world in ways that resist technical, space-centric descriptions, and technical and space-centric cyber actor models will not adequately predict their behavior. As seen in the following analysis, the cyber tribe model shows predictive promise by connecting place to cyber tribe leadership, decision making, and internal structure.

The egalitarian structure bequeathed to Anonymous from 4chan also gave rise to the group's tribal system of leadership, which in turn influences its decisions to engage in raids. Similar to the Yanomami tribe of South America (and many others), Anonymous does not maintain a strict leadership hierarchy.[34] The Yanomami employ headmen who influence tribal decisions, but they do not exert authority. Because the headmen do not exert authority, they must build a raiding party from volunteers.[35] In Anonymous, the raiding system relies on ad hoc parties formed by influencers and organizers.[36] The cyber-persona equivalent of a Yanomami headman would advertise a particular raid on 4chan, then provide a link to a more private IRC channel to plan the details.[37] Just like the Yanomami,[38] not everyone who joined the chat would be required to complete the raid.

The reasons for raiding also follow the trend of tribal warfare. Anonymous conducts raids for at least three reasons: lulz, violation of their tribal values/norms, and revenge. Lulz is a

malformed version of LOL (an abbreviation for "laughing out loud") and generally means pranking someone to derive pleasure from their embarrassment.[39] Lulz is a difficult motivation for the military strategist to understand, but it makes sense within the context of Anonymous' culture. Anons raid for lulz with an audience of other Anons in mind,[40] so raiding provides social capital to the prankster while sustaining the larger Anonymous community. A similar and similarly mystifying mechanic occurred with the practice of scalp taking by Pawnee war bands. Misunderstood as a simple trophy system for many years,[41] scalping was intricately bound up in Pawnee spiritual belief. Taking a scalp provided spiritual power, which increased the social standing of the scalp taker as well as sustaining the power of his community.[42] Because 4chan is partly based on unfettered access to entertainment and Anonymous thrives on media attention, collecting lulz raises the perpetrator's social standing while sustaining 4chan and Anonymous' collective fame. Gabriella Coleman described the aftermath of a major raid this way:

> For days following this epic showdown, the lulz pulsed through the IRC chat channels, electrifying and recharging the collective mood. The press could not get its fill of the hack.[43]

As the Pawnee's scalping practice sustained the larger tribe, Coleman's account describes the literal sustainment of Anonymous through lulz.

Anonymous might also choose to raid a site or individual for violating the group's norms and values. Anonymous' value of anonymity, for example, resembles the Yanomami practice of having both a privately-held sacred name and a public name. In Yanomami culture, knowing a person's sacred name gives the speaker power over the named person, and sharing one's sacred name with outsiders is considered taboo.[44] Uncovering or revealing an Anon's non-cyber identity is also taboo. Anonymous expects members to hide their identifying technical information and not talk about themselves in online forums. On 4chan, Anons forbid the mention of age, race, or

gender.[45] Revealing a non-cyber identity, like a sacred name, provides power over the named person. It opens them to pranks by other Anons (for the lulz), but also opens them to arrest and prosecution for crime committed under the Anonymous banner. Attempts to uncover Anons' offline identities can garner an unpleasant response. When security consultant Aaron Barr attempted to connect Anons' cyber-personas with their non-cyber identities in 2011, for example, Anonymous destroyed Barr's reputation as well as his employer's business and side projects.[46] The ferocity and completeness of the attack underscores how strongly some Anons adhere to the group's cultural norms and values.

Also like the Yanomami, Anonymous resorts to warfare to exact revenge. In Yanomami culture, seeking revenge against the original perpetrator is desirable, but not required. Attacking a member of the perpetrator's group usually suffices.[47] Anonymous responded to the January 2015 attacks on employees of the French magazine Charlie Hebdo with a video declaring a campaign of revenge against ISIS, Al Qaida, and "other terrorists."[48] It did not matter that the perpetrators were unavailable for retribution or that their parent terrorist organization remained unconfirmed. Like the Yanomami, Anonymous satisfied their revenge by striking in the general vicinity of the perpetrators' group and taking down a seemingly unrelated extremist website.[49] The similarity between Yanomami and Anonymous modes of warfare further suggests that studies of tribal warfare provide a fruitful starting place to understanding cyber tribes.

While Anonymous may appear opaque and amorphous to outsiders, the group actually encourages this perception through tribal patterns of behavior. Anonymous, like various real-world tribes, draws cultural boundaries through argot, atrocity, and leveling. Argot is specialized language or slang intended for exclusive use within a small cultural group. Membership in the cultural group requires understanding and mastery of this specialized language. As Coleman

points out, the term "lulz" is an example of argot. Those seeking to LOL are divided from those looking for lulz. Crossing the cultural barrier into Anonymous membership requires access to this knowledge.[50] Other examples of Anonymous' argot include, "cheese pizza," "moar," "moralfag,"[51] and "namefagging."[52]

The argot term "cheese pizza" hints at Anonymous' tribe-like use of atrocity to create cultural barriers. Tribal warriors in Papua New Guinea would collect heads from enemy tribes and use them to decorate their home village. Committing this atrocity serves as a warning and deterrent against any potential threats from outsiders.[53] Anonymous uses similar methods to discourage incursion by outsiders. On 4chan and in Anonymous culture "cheese pizza" refers to child pornography in an obscenely humorous way.[54] Mainstream Western culture reviles child pornography and including such "humorous" content effectively deters many outsiders from delving more deeply into Anon culture.[55] Anonymous-related message boards on 4chan also construct additional cultural barriers between tribal and mainstream society with homophobic, racist, and misogynistic content.[56]

The term "namefagging," an example of argot and homophobic atrocity, points to tribe-like leveling mechanisms. When a hunter from the African !Kung tribe catches large quantities of game, his fellow tribespeople ridicule his achievement instead of providing praise. The ridicule socially smooths power differences and enforces the tribe's egalitarian structure.[57] Elizabeth Cashdan identifies the !Kung's leveling practices as a form of social insurance. Enforcing an egalitarian social structure pools the tribe's risk against an unsteady food supply.[58] Namefagging is a taboo behavior wherein an Anon attempts to parlay their in-tribe fame into mainstream fame by crediting exploits to either their cyber-persona or real-world identity.[59] The namefagging taboo helps enforce Anonymous' egalitarian structure, and, like the !Kung,

represents a form of social insurance. Instead of food supply, Anons engaged in illegal activity face the uncertain risk of investigation and arrest. Disconnecting exploits from individual identities pools the group's risk of arrest while the *decision* to pool risk helps define a cultural line between tribe and other.

Limits of the Cyber Tribe Model

In modeling non-state cyber actors, cyber tribes will never fully mirror tribes in real life. There are aspects of tribal life which do not currently translate to a cyber analog. Physical bodies do not exist in cyberspace, so cyber tribes are unlikely to organize based on kinship networks or strengthen inter-tribal relationships through marriage. By the same reasoning, patterns of sustenance and health are unlikely to apply. Despite these differences, the tribal cultural model creates a starting point for thinking about complex non-state cyber actors. It borrows from anthropology, a mature field with a long history of studying groups operating outside of state authority. Cyberspace presents a similarly ungoverned space—at least, from the state's perspective. Thinking of complex non-state cyber actors as tribes provides valuable operational lessons precisely because it offers a non-state perspective.

Operational Implications

Effective targeting in cyberspace will require the military to identify relevant cyber places. Differences between state and non-state cyber actors drive the need to simplify target sets. A state-sponsored cyber actor may arrange its cyber assets to mirror its physical world organization. For example, an Air Operations Center (AOC) represents a critical friendly node for the US Air Force. The cyber systems supporting an AOC constitute an equally important node for adversaries since disabling its cyber systems may also disable the AOC. Cyber planners cannot rely on the same correlation for cyber tribes like Anonymous. Since cyber tribes exist

primarily within cyberspace, planners will not observe physical world assets (like an AOC) which point them to related cyber targets. The sheer number of dispersed systems may overwhelm planners as well. During operations supporting WikiLeaks, Anonymous offered the cyber attack tool "Low Orbit Ion Cannon" as a free software download. The tool was downloaded 116,988 times in a single month, creating thousands of potential targets for cyber operations. Whether from lack of physical analogs or sheer numbers, identifying cyber places reduces the complexity of targeting by focusing effort on what most influences *human behavior* in cyberspace.

Dr. Casey's philosophical model of place will also help strategists develop centers of gravity (COGs). As mentioned previously, the influence of places can be measured by their habitudinal density. Discovering, documenting, and tracking habitudes and habitation in the physical world takes a significant investment of effort. Anthropologists accomplish this during field work and immersion with tribal cultures. Digital communication, however, is inherently recordable. As Gold found in his study of the MSC-L disability support group, textual information carried the most significant evidence of culture and cyber place.[60] Recording and analyzing this information would reveal cyber-persona habitation patterns and whether a given cyber place shapes those personas' habitudes. The thickest places would then top the list of potential COGs.

Should COG analysis prove fruitless, the cyber place concept helps predict cyber tribal reactions to proposed military actions. Tribal cultures often associate tribal existence as inseparable from place. A tribe would likely perceive a threat to place as an existential threat. Any state-sponsored cyber actor (military, law enforcement, or otherwise) should expect a

warlike response to censuring 4chan, for example. Keeping situational awareness of cyber places may help planners anticipate a counterattack or prevent unintended conflicts.

The inextricable relationship between persona and cyber place offers operational approaches not available from a space-centric view. Instead of influencing or attacking the disparate technical resources that support the representation of persona in cyberspace, operators may influence the habitus of integrated personas by manipulating cyber place. Operations can affect the meaning of a place without much regard for its technical terrain. Flooding a thick cyber place with norm-violating personas, for example, might attenuate habitudinal density or shape the habitus of existing members. Conducting information operations within the context of cyber place may also be able to separate individual personas from place without affecting individuals' rights in the physical world. Influencing cyber-personas versus people in the "real world" is an important distinction that may have bearing on the legality of future cyber operations.

Treating Anonymous and similar groups as cyber tribes also provides lessons to military doctrine on cyber actor motivation and behavior prediction. First, doctrine should recognize that, like real-world tribes, cyber tribes may not have an authoritative leader. Arresting, killing, or isolating any member of a cyber tribe may not degrade the tribe's overall strength and may even invite a retaliatory raid. Second, doctrine should seriously consider how to influence a cyber tribe via their values and norms. Lulz may sound like a silly concept to a military strategist, but denying opportunities for lulz through security and strategic communications may be the best way of influencing Anonymous' behavior or degrading its membership base. Other non-state cyber actors may have similarly mystifying motivations. Codifying in joint doctrine the requirement to identify community-sustaining practices, like Anonymous lulz or Pawnee

scalping, will help military cyber strategists predict which cyber tribes pose a threat and what courses of action threatening tribes are likely to take during conflicts.

Finally, Anonymous and the cyber tribe model point to the cultural difficultly military cyber strategists will face in studying complex, non-state cyber actors. The Air Force values a professional workplace that strictly prohibits racism, sexism, lewd material, and most forms of discrimination. How then do strategists or planners remain culturally competent regarding cyber tribes when it may require them to openly discuss argot that runs counter to their professional ethic? When cyber tribes employ atrocity to create cultural barriers, how will planners remain focused on military objectives and not become emotionally distraught by lurid content? How will serious-minded senior leaders respond when a staffer proposes lulz as a cyber actor's motivation? Meeting these challenges requires new levels of cultural relativism—the understanding of a "culture or a cultural trait through the perspective of someone within that culture."[61] The cyber tribe model provides a means for exercising cultural relativism in cyberspace by placing complex, non-state actors within the context of the long established field of anthropology.

Conclusion

Anonymous is a complex cyber actor that exhibits many elements of a tribal culture. It represents a new class of cyber actor that derives meaning from place, follows an influence-based leadership model, and conducts war for reasons not readily understood by modern nation-states. Like ISIS and other complex actors, Anonymous challenges the usefulness of contemporary military doctrine. A comparison between Anonymous' cultural features and those of non-cyber tribes shows how military strategists can apply the cyber tribe concept as a starting point for understanding complex, non-state cyber actors. The US military should update doctrine

to recognize the role of place, values/norms, community sustainment mechanisms, and motivations in planning operations that affect cyber tribes and their indigenous cyber-personas. Only then can cyber strategists exercise the required amount of cultural relativism needed to influence complex, and sometimes disturbing, non-state cyber actors.

Endnotes

[1] Keely Lockhart, "'Hacktivist' Group Anonymous Says It Will Avenge Charlie Hebdo Attacks by Shutting down Jihadist Websites," *The Telegraph*, 10 January 2015, http://www.telegraph.co.uk/news/worldnews/europe/france/11335676/Hacktivists-Anonymous-says-it-will-avenge-Charlie-Hebdo-attacks-by-shutting-down-jihadist-websites.html.
[2] Gabriella Coleman, *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous* (Brooklyn, NY: Verso Books, 2014), 8.
[3] David Kushner, "An Inside Look at Anonymous, the Radical Hacking Collective," *The New Yorker*, 8 September 2014, http://www.newyorker.com/magazine/2014/09/08/masked-avengers.
[4] Coleman, *Hacker, Hoaxer, Whistleblower, Spy*, 173-176.
[5] Parmy Olson, *We are Anonymous: Inside the Hacker World of LulzSec, Anonymous, and the Global Cyber Insurgency* (New York: Little, Brown and Company, 2012), 26-28.
[6] Coleman, *Hacker, Hoaxer, Whistleblower, Spy*, 4-8.
[7] Ibid, 96.
[8] Ibid, 126.
[9] Curtis E. LeMay Center for Doctrine Development and Education, "Annex 3-12 Cyberspace Operations," 30 November 2011, 3-4.
[10] Joint Publication (JP) 3-12R, *Cyberspace Operations*, 5 February 2013, v.
[11] Ibid, vi.
[12] Ibid, I-4.
[13] Brian R. Ferguson, "Tribal Warfare," in *The Encyclopedia of War*, ed. by Gordon Martel (Blackwell Publishing Ltd., 2012), 1.
[14] "Tribe and Tradition in the Modern Context" (lecture, Air Command and Staff College, Maxwell AFB, AL, 18 February 2015).
[15] Edward S. Casey, *The Fate of Place: A Philosophical History* (Berkeley, CA: University of California Press, 1997), 77.
[16] Amanda Kearney and John J. Bradley, "'Too Strong to Ever Not Be There': Place Names and Emotional Geographies," *Social & Cultural Geography* 10, no. 1 (2009): 77-79.
[17] Olson, *We Are Anonymous*, 28.
[18] Ibid, 34.
[19] Ibid, 34, 49.
[20] Ibid, 29.
[21] Edward S. Casey, "Between Geography and Philosophy: What Does It Mean to Be in the Place-World?" *Annals of the Association of American Geographers* (2001): 685.
[22] Ibid, 686.
[23] Ibid, 687.
[24] Olson, *We Are Anonymous*, 29-31.
[25] Casey, "Between Geography and Philosophy," 686.
[26] Gerald Gold, "Rediscovering place: experiences of a quadriplegic anthropologist," *The Canadian Geographer/Le Géographe Canadien* 47, no. 4 (2003): 474.
[27] JP 3-12R, *Cyberspace Operations*, I-4.
[28] Coleman, *Hacker, Hoaxer, Whistleblower, Spy*, 184-189.
[29] Ibid, 363.

[30] Maureen Trudelle Schwarz, "Snakes in the ladies' room: Navajo views on personhood and effect," *American ethnologist* 24, no. 3 (1997): 602.
[31] Coleman, *Hacker, Hoaxer, Whistleblower, Spy*, 362-363.
[32] John L. Comaroff and Jean Comaroff, "On personhood: an anthropological perspective from Africa," *Social Identities* 7, no. 2 (2001): 275-276.
[33] Olson, *We Are Anonymous*, 410.
[34] Ibid, 58-59.
[35] Napoleon A. Chagnon, "Life Histories, Blood Revenge, and Warfare in a Tribal Population," *Science* 239, no. 4843 (1988): 987.
[36] Olson, *We Are Anonymous*, 58-59.
[37] Ibid, 50-52.
[38] Chagnon, "Life Histories, Blood Revenge, and Warfare," 987.
[39] Olson, *We Are Anonymous*, 478.
[40] Coleman, *Hacker, Hoaxer, Whistleblower, Spy*, 237.
[41] Mark van de Logt, "'The Powers of the Heavens Shall Eat of My Smoke': The Significance of Scalping in Pawnee Warfare," *The Journal of Military History* 72, no. 1 (01, 2008): 71-75.
[42] Ibid, 80-82.
[43] Coleman, *Hacker, Hoaxer, Whistleblower, Spy*, 229.
[44] "Tribe and Tradition in the Modern Context."
[45] Olson, *We Are Anonymous*, 34.
[46] Ibid, 3-25.
[47] Chagnon, "Life Histories, Blood Revenge, and Warfare," 985.
[48] Lockhart, "'Hacktivist' Group Anonymous."
[49] Harriet Line, "Charlie Hebdo Attack: Anonymous Claims First Victory in 'war' on Jihadi Websites," *The Telegraph*, 12 January 2015, http://www.telegraph.co.uk/news/worldnews/europe/france/11340040/Charlie-Hebdo-attack-Anonymous-claims-first-victory-in-war-on-jihadi-websites.html.
[50] Coleman, *Hacker, Hoaxer, Whistleblower, Spy*, 31.
[51] Olson, *We Are Anonymous*, 33-34.
[52] Coleman, *Hacker, Hoaxer, Whistleblower, Spy*, 189.
[53] "Tribe and Tradition in the Modern Context."
[54] Olson, *We Are Anonymous*, 33-34.
[55] Coleman, *Hacker, Hoaxer, Whistleblower, Spy*, 42.
[56] Olson, *We Are Anonymous*, 29-34.
[57] Coleman, *Hacker, Hoaxer, Whistleblower, Spy*, 189-190.
[58] Elizabeth A. Cashdan, "Egalitarianism among hunters and gatherers," *American Anthropologist* 82, no. 1 (1980): 116-117.
[59] Coleman, *Hacker, Hoaxer, Whistleblower, Spy*, 184-189.
[60] Gold, "Rediscovering place," 475.
[61] "Tribe and Tradition in the Modern Context."

Bibliography

Casey, Edward S. "Between Geography and Philosophy: What Does It Mean to Be in the Place-World?" *Annals of the Association of American Geographers* (2001): 683-693.

Casey, Edward S. *The Fate of Place: A Philosophical History*. Berkeley, CA: University of California Press, 1997.

Cashdan, Elizabeth A. "Egalitarianism among hunters and gatherers." *American Anthropologist* 82, no. 1 (1980): 116-120. http://www.jstor.org/stable/676134.

Chagnon, Napoleon A. "Life Histories, Blood Revenge, and Warfare in a Tribal Population." *Science* 239, no. 4843 (1988): 985-992.

Coleman, Gabriella. *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous*. Brooklyn, NY: Verso Books, 2014.

Comaroff, John L., and Jean Comaroff. "On personhood: an anthropological perspective from Africa." *Social Identities* 7, no. 2 (2001): 267-283.

Curtis E. LeMay Center for Doctrine Development and Education. "Annex 3-12 Cyberspace Operations," 30 November 2011. https://doctrine.af.mil/download.jsp?filename=3-12-Annex-CYBERSPACE-OPS.pdf.

Ferguson, Brian R. "Tribal Warfare." In *The Encyclopedia of War*. Edited by Gordon Martel. Blackwell Publishing Ltd., 2012.

Gold, Gerald. "Rediscovering place: experiences of a quadriplegic anthropologist." *The Canadian Geographer/Le Géographe Canadien* 47, no. 4 (2003): 467-479.

Joint Publication (JP) 3-12R. *Cyberspace Operations*. 05 February 2013.

Kearney, Amanda, and John J. Bradley. "'Too Strong to Ever Not Be There': Place Names and Emotional Geographies." *Social & Cultural Geography* 10, no. 1 (2009): 77-94.

Kushner, David. "An Inside Look at Anonymous, the Radical Hacking Collective." *The New Yorker*. 8 September 2014. Accessed 1 April 2015. http://www.newyorker.com/magazine/2014/09/08/masked-avengers.

Line, Harriet. "Charlie Hebdo Attack: Anonymous Claims First Victory in 'war' on Jihadi Websites." *The Telegraph*. 12 January 2015. Accessed 1 March 2015. http://www.telegraph.co.uk/news/worldnews/europe/france/11340040/Charlie-Hebdo-attack-Anonymous-claims-first-victory-in-war-on-jihadi-websites.html.

Lockhart, Keely. "'Hacktivist' Group Anonymous Says It Will Avenge Charlie Hebdo Attacks by Shutting down Jihadist Websites." *The Telegraph*. 10 January 2015. Accessed 28 March 2015. http://www.telegraph.co.uk/news/worldnews/europe/france/11335676/Hacktivists-Anonymous-says-it-will-avenge-Charlie-Hebdo-attacks-by-shutting-down-jihadist-websites.html.

Logt, Mark van de. "'The Powers of the Heavens Shall Eat of My Smoke': The Significance of Scalping in Pawnee Warfare." *The Journal of Military History* 72, no. 1 (01, 2008): 71-104. http://search.proquest.com/docview/195634675?accountid=4332.

Olson, Parmy. *We are Anonymous: Inside the Hacker World of LulzSec, Anonymous, and the Global Cyber Insurgency*. New York: Little, Brown and Company, 2012.

Schwarz, Maureen Trudelle. "Snakes in the ladies' room: Navajo views on personhood and effect." *American ethnologist* 24, no. 3 (1997): 602-627.

"Tribe and Tradition in the Modern Context." Lecture. Air Command and Staff College, Maxwell AFB, AL, 18 February 2015.