Title:

A Typology of Hackers: Classifying Cyber Malfeasance using a Weighted Arc Circumplex Model

Author Name:

Ryan Seebruck

seebruck@email.arizona.edu

+16083770951

Author Affiliation:

University of Arizona, School of Sociology

Abstract

Cyber attacks continue to increase in frequency and variety, making cyber malfeasance a rising area of study and a major policy issue. Categorizing cyber attackers aids targeted organizations in efficiently directing resources to enhance security. However, extant hacker typologies do not fully account for the multifaceted nature of cyber malfeasance, including the rise in socially and ideologically motivated hacking (e.g. crowdsourcing, hacktivism). I clarify the current state of field by uniting recent case studies on hackers with existing categorization techniques. Previous researchers have employed circumplex models—visualizations which depict relationships and boundaries between groups—as a way to visually organize hacker types. I propose an updated model—a weighted arc circumplex model—that is designed to represent the multidimensional nature of contemporary hacker types by offering a means of visually representing multiple motivations simultaneously. Finally, I demonstrate how archetypical circumplex models can be wed with sociograms to depict social and technical relationships between hacker groups.

Keywords: digital forensics, hackers, cyber crime, circumplex, typology, taxonomy, sociogram

Introduction

“[C]yberattacks have the potential to destabilize on a global scale. Cybersecurity must therefore be a matter of global concern.”

- Secretary-General of the United Nations Ban Ki-moon (October 2013)

With everyday operations in nearly every sector of society increasingly dependent on networked computers, the stability of the global economic, social, and political systems depends on the efficient functioning of internet and intranet systems. The U.S. government emphasizes the importance of cyber security, holding annual congressional meetings on the topic, publishing dozens of reports annually, and issuing numerous executive orders on the issue (Tehan, 2013). Cyber security is therefore a serious policy issue requiring the cooperation of all legitimate players in cyber space, particularly governments and corporations that own or govern cyber infrastructure (Obama, 2013).

Despite government focus on cyber security, global cyber space remains vulnerable and cyber malfeasance is increasing (Rogers, 2010; Wilshusen, 2011). Every day British Petroleum fends off 50 thousand cyber attacks whereas the Pentagon receives 10 million (Glenny, 2013). These cyber attacks create serious monetary damages. In 2012, credit card hackers stole \$11.5 billion; in 2013 one ATM heist garnered \$40 million in ten hours (Glenny, 2013). Even failed cyber intrusions create collateral damage that requires time and money to fix. Estimates of global losses from cyber attacks range from \$120 billion to \$1 trillion annually (Glenny, 2013).

The rise in cyber malfeasance led the U.S. government to issue a series of executive orders calling for improved cyber security (Obama, 2013, 2015a, 2015b). The most recent one labels cyber malfeasance a “national emergency” and a “significant threat” to national security, foreign policy, economic health, and financial stability (2015b:1). A common policy goal delineated in these executive orders is to improve cyber security by sharing information so as to help targets of cyber attacks mitigate risks. As the U.S. Congress reports that cyber threats stem from “multiple sources” using a “variety of attack techniques” (Wilshusen, 2011:3), one strategy for achieving such cyber security goals is to improve methods for classifying cyber attackers.

A useful approach to classifying cyber attackers is to create a typology, which enables cyber security analysts to more efficiently identify threats based on known hacker types. Typologies improve

our understanding of adversaries but are difficult to create, particularly for cyber adversaries, whose identities are often concealed by the anonymous nature of computer-mediated communication (Rogers, 2010). Thus, a significant challenge facing the cyber security industry is ascertaining who the perpetrator is and what they are capable of doing (Glenny, 2013). The challenge stems from the broad range of cyber attackers, composed of various types with differing capabilities and motivations. Categorizing the motivations behind, and techniques used in, cyber attacks helps targeted organizations lower security costs by facilitating their ability to quickly direct resources to combat attacks (Buyens, De Win, and Joosen, 2007; Farahmand, Sharp, and Enslow, 2005).

However, existing hacker typologies do not thoroughly account for the rise in socially and ideologically motivated hacking (e.g. crowdsourcing, hacktivism), two types of motivations that are characteristic of modern hacking. Nikitina (2012) illustrates this point, noting the rise of hacking as a "social phenomenon"—the product of youth growing up in an evolving digital culture with a desire to subvert—and this can be seen in recent increases in ideologically and socially motivated cyber activity such as hacktivism and crowdsourcing. As typologies should continue to grow and be refined over time (Mirkovic and Reiher, 2004), I seek to summarize the recent discussions and case studies about hackers and cyber security and then wed this information with past categorizations of hackers to provide a unified and updated view of this subfield.

To visually depict this, I draw from previous hacker typologies by employing circumplex models: visualizations consisting of a circle with axes to define boundaries between groups (Rogers, 2006, 2010). Circumplex models have been adapted from psychology by sociologists seeking to classify groups according to attributes—what Lindqvist and Jonsson (1997:157) call “dimensions”—such as classifying hacker types by placing nodes in sectors that represent motivations. However, using nodes suggests single or dual motivations since nodes can only be placed in one sector (or on the border of two). In reality, hackers are driven by multiple motivations. Consequently, I replace nodes with arcs and

proportionally weight them by motivational intensity, which offers increased flexibility in categorizing groups.

This adapted model, which I call a weighted arc circumplex model, is able to capture multiple motivations because arcs can cross through multiple sectors in the circumplex model. Weighting them reveals motivational intensity, with the thickest arc segment indicating a group's primary motivation and proportionally thinner segments indicating secondary, tertiary, quaternary, or quinary motivations, if applicable. Thus, in contrast to past typologies, the weighted arc circumplex model proposed here is designed to represent the multidimensional nature of hackers' motivations and capabilities, and is therefore suited to represent the current state of cyber malfeasance.

What Typologies Are and Why They Are Needed

Before discussing the models used to categorize hackers, it is important to relate the types of categorization tools and their benefits. There are two basic types of classification: typologies and taxonomies (Smith, 2002). Often these terms are used interchangeably by researchers, but, there are nuances. In a typology, the key trait is that dimensions depict concepts—that is, ideal types—rather than empirical cases, meaning typologies are not necessarily exhaustive. Taxonomies differ in that they categorize dimensions based on empirical observation and measureable traits (Bailey, 1994). Consequently, taxonomies tend to be more associated with the biological sciences whereas typologies are more common in the social sciences (Smith, 2002; Sokal and Sneath, 1964). Given that the models here are meant to be ideal types based on qualitative data, I refer to them as typologies. However, some of the literature cited below uses the term taxonomies instead.

Regardless of the name, classifying phenomena has many purposes that can benefit administrators of critical infrastructures like computer networks that are at risk of being attacked. In their essay on crisis management, Boin and McConnell (2007) note the importance of preparedness to maximizing predictability as a strategy for containing emergencies. This is especially crucial given the

complexity and tight coupling of critical infrastructure systems, where even minute disruptions can escalate quickly (Perrow, 1999; Turner, 1978), compounding emergencies into crises, crises into disasters, and disasters into catastrophes (Boin and McConnell, 2007).

Boin and McConnell assert that preparing for all threats is "simply impossible" (2007:52), even before considering the resource constraints most organizations face. The solution is risk management: reducing the "multitude of threats by discarding low priority ones" (Buyens, De Win, and Joosen, 2007:1). Here, risk is the impact, or cost, of a threat happening multiplied by the odds of it occurring. For the same reason that landlocked areas need not waste resources preparing for hurricanes, neither should organizations waste resources preparing against unlikely threats. Thus, the goal of any administrator of critical infrastructure should be "to mitigate risk in a cost-effective fashion, not to eliminate risk entirely" (Friedman and Hoffman, 2008:175).

Categorizing threats is one such risk management strategy. In their analysis of threat management techniques, Buyens et al (2007:4) assert that one of most cost-efficient risk management strategies is to develop "attacker profiles" which disclose the skill-level of likely attackers. Likewise, in discussing the management of security threats to information systems, Farahmand et al (2005:204) also proclaim the necessity of an "organized classification that helps our understanding of threats" and therefore aids managers in determining how much time and money should be spent on what types of cyber security strategies. Likewise, while simulating computer security intrusions, Lindqvist and Jonsson (1997) realized a need for a classification system, arguing that categorization enables the compilation of statistics, which can then be used to predict intrusions and therefore strengthen systems against future intrusions. Furthermore, they contend that an established taxonomy facilitates reporting of incidents, which is important because detailed records of intrusions over time can make known new security flaws, helping organizations stay ahead of quickly evolving cyber threats.

In sum, categorization has several benefits: it makes possible systematic studies, it helps managers build efficient defense systems that are less vulnerable without wasting resources on unlikely threats, and it facilitates the reporting of incidents to relevant response teams (Farahmand et al, 2005). Finally, typologies of cyber security threats in particular are beneficial to IT professionals, executive managers, academics, and anyone concerned with the security of digital information and critical infrastructures in that they ensure that classes of threats are not overlooked, make clearer the types of threats of each class, and enable security agents to assess the relative risks of these threats and prioritize addressing them (Friedman and Hoffman, 2008). This is especially crucial with cyber deviancy, where there is a tendency to lump together various cyber deviants under the nebulous umbrella term 'hacker' even though there is great variation in the capabilities and motivations of hackers (Seigfried-Spellar and Treadway, 2014).

Earlier Hacker Typologies

Given the usefulness of categorizing cyber threats, such typologies have a long history. Academic discussions of cyber adversaries began in the 1980s, when personal computers entered the mainstream, and with that, the concomitant realization that skilled individuals could manipulate computer systems (Meyers et al, 2009). While initially used to describe anyone capable of computer manipulation, the term 'hacker' came to refer to individuals engaging in malicious behavior. The media have exacerbated the issue by frequently using the historically benign word 'hacker' interchangeably with the word cyber criminals (Rogers, 2010). Although many view this as a misuse of the word 'hacker', preferring the term 'cracker' instead (Lawson, 2001), mass usage deems as hacker anyone who infiltrates a computer system, regardless of motivation or the extent of the damage caused.

As cyber intrusions increased in the 1990s and 2000s so did the attention of lawmakers, law enforcement, and scholars, who sought to classify hackers to facilitate the identification of and motivations behind cyber attackers (Rogers, 2006). Rather than lumping together cyber adversaries

under the umbrella term hacker, Rogers (2006) argues that, to aid our understanding of cyber malfeasance, a broader taxonomy is needed to provide a clearer picture of hackers' motives.

One early attempt to classify hackers is that of Landreth (1985), who proposes five types of hackers based on skill and motivation (mischief, intellectual challenge, thrill, ego boost, and criminal profit). In comparison, Hollinger (1988) classifieds hackers only by skill whereas Chantler (1996) categorizes them according to motivation, ability, and experience. Ideally, we could distinguish cyber attacks based on several parameters such as "the identity of the perpetrators and the target, the method and frequency of occurrence, the goal to be attained, and the damage caused" (Vegh, 2003:82). But, because such data are rarely available, it is more realistic to adopt a parsimonious categorization scheme such as Rogers's (2006, 2010), which classifies hackers based on skill and motivation (revenge, financial, notoriety, and curiosity).

While the parsimony of Rogers's (2006) taxonomy is preferable to previous ones, which utilized more complex categorization schemes (e.g. Chantler, 1996), recent shifts in cyber malfeasance warrant an opportunity to build upon his work by highlighting ideology as a motivation. While previous studies encompass a wide range of potential motivations for hacking (see McBrayer, 2014)—such as addiction, curiosity, entertainment, money, power, status, or revenge—few emphasize ideology as its own category (c.f. Holt, 2009). For instance, in noting the general paucity of research devoted to understanding the motivations behind cyber attacks, Holt (2009) laments the dearth of studies that consider ideological motivations such as nationalism or religion. Whereas Rogers (2006, 2010) acknowledges political activists as a hacker type, the recent increase in ideologically motivated hacking (Egan, 2011; Glenny, 2013) reveals the need for an updated taxonomy that more fully emphasizes the rise in cyber activists.

Using Rogers's (2006) four motivations— revenge, financial, notoriety, and curiosity—as a foundation, Meyers et al (2009) offer an updated taxonomy that formally specifies political activists, or

'hacktivists', as a category of hackers. Although an improvement, ultimately their efforts are misplaced by forcing hacktivists into the notoriety group without explanation. Rogers's (2010:219) updated taxonomy, while formally identifying hacktivists as class of cyber adversaries, also places them in the notoriety category, arguing that political motivation is not usually the primary motivation of hacktivists, despite hacktivists' claims. Instead, he suggests that they may belong to other hacker types and are merely using ideology as "semantic camouflage" to disguise their behavior.

However, recent case studies of prominent hacktivist groups has revealed that hacktivists are a unique class of cyber adversaries and that ideology is an important motivational driving their activity (Pendergrass, 2013). As hacktivists are more so motivated by ideology than by notoriety (Glenny, 2013; Vegh, 2003), an updated hacker typology that more fully emphasizes the role of ideology and hacktivism could benefit cyber defense systems. The need for an updated typology is further evident by the rise of another important hacker type: social cyber malfeasance known as crowdsourcing, a hacker type not covered by Rogers (2006, 2010) or Meyers et al (2009). Following that, I propose that the motivations propelling hackers be modified to reflect the recent increase in ideologically (Egan, 2011; Glenny, 2013) and socially (Wang et al, 2010) motivated cyber attacks.

An Updated Hacker Typology

Earlier hacker typologies no longer capture the broad range of contemporary hackers necessary to combat cyber malfeasance today. As the Internet has become more mainstream the composition of its users has diversified, and with this more diverse population comes a more diverse spectrum of cyber activity, including a broader array of hackers with a wider range of skills and motivations.

Two types of cyber actors that have recently rose to prominence are hacktivists and crowdsourcers. Hacktivists are motivated by ideology, such as politics, religion, or jingoism. As an example of this, in 2005 religiously motivated Turkish hackers defaced Danish websites that published a political cartoon of the prophet Muhammad (Holt 2009). Anarchists who manipulate computer systems

to further their political beliefs also fall under the hacktivist umbrella. Online crowdsourcing movements consist of collective efforts to solve a problem, sometimes using questionable methods or in pursuit of dubious goals. It is worth noting that there are many legitimate and legal instances of crowdsourcing; this paper is focused on dubious instances instead, such as those that involve ‘doxing’: using Internet resources, including hacking into social media accounts, to research and broadcast personally identifiable information about an individual. One example of this type of crowdsourcing is the concept of human flesh search in China, where Web users unite to identify corrupt government officials (Wang et al, 2010). A revised typology of hackers that includes ideologically and socially driven online activism more accurately captures the current state of hacking.

Indeed, despite improvements in recent hacker typologies, Glenny (2011:268), in his examination of contemporary credit card hackers, calls for an increase in research aimed at “trying to ascertain who is hacking and why.” Glenny argues that contemporary reports on cyber malfeasance do not differentiate between “hackers from WikiLeaks, from the American or Chinese military, from criminal syndicates and from the simply curious” even though the skills, targets, and motivations of these groups differ (268). Glenny concludes that understanding the skills and motivations of cyber adversaries “would enormously benefit a security industry that is over-dependent on technical solutions” (269).

I therefore propose a hacker typology that captures the recent increases in ideologically and socially motivated hacking (Egan, 2011; Glenny, 2013; Wang et al, 2010). In line with previous research (Landredth, 1985; Meyers et al, 2009; Rogers, 2006, 2010), I categorize hackers by skill and motivation. Rogers’s (2006, 2010) and Meyers et al’s (2009) taxonomies were based on four motivations: curiosity, notoriety, revenge, and financial gain. Given recent additions to the literature on hacking, I add a fifth motivation—ideology—and reclassify the other four as recreation, prestige, revenge, and profit. *Ideology* encompasses political activists (those motivated by contemporary social issues) as well as

nationalists (attacks initiated by patriotic civilians or state-sponsored cyber warfare). *Recreation* covers those who hack for pleasure, such as intellectual curiosity, thrill, or mischief. *Prestige* is for non-material gains such as notoriety and is the primary motivation of non-malicious coders (e.g. white hat hackers). *Profit* is for material gain (e.g. money) and is the primary motivation for criminals. *Revenge* comprises both personal vengeance (e.g. inside jobs by disgruntled workers) and larger social justice issues (e.g. online crowdsourcing movements).

The Modified Circular Order Circumplex Model

Circumplex models are used to present different concepts and the relations between them, such as how Rogers (2006, 2010) employed a modified circular order circumplex to categorize archetypal groups of hackers. In his modified circular order circumplex, a circle is divided into four quadrants, each representing a motivation. Position in a modified circular order circumplex is important: groups positioned near each other are related, positions close to quadrant edges indicate overlapping motivations, and positions farther from the center indicate increased technical skills. Using a circular order circumplex model to categorize hackers is a useful way to depict the relationship between hackers' motivations and skills, which facilitates the identification of cyber adversaries by enabling analysts to more quickly categorize hackers (Rogers, 2006) and therefore more efficiently direct resources to address a cyber attack (Buyens, De Win, and Joosen, 2007; Farahmand, Sharp, and Enslow, 2005).

To reflect the current state of this subfield, I build on the hacker typologies posited by Rogers (2006, 2010) and Meyers et al (2009), adding in a new category of cyber actors—crowdsourcers—while providing greater emphasis on the hacktivist category. This results in a typology composed of eight hacker types, listed in ascending order of technical expertise: *novices*, *crowdsourcers*, *punks*, *hacktivists*, *insiders*, *criminals*, *coders*, and *cyber warriors*. These groups are described below. Following Rogers (2006, 2010) and Meyers et al (2009), I plot these hacker types on a modified circular order circumplex model according to motivation and sophistication but with the added motivation of ideology (see Figure

1). Each of the five motivations has its own sector in the circumplex model: ideology, recreation, prestige, revenge, and profit. The data and methods used to create these models are described below. Recall that position in a circular order circumplex model indicates relationship, so that nearby groups are more closely related, positions near sector boundaries indicate multiple motivations, and positions closer to the outer edges of the circle indicate more sophisticated hackers—that is, those who employ more advanced techniques.

[Insert Figure 1 about here]

In Figure 1, the position of *hacktivists* indicate attackers of lower-intermediate skill level who are primarily motivated by political ideology. The position of *cyber warriors* indicates highly sophisticated attackers motivated by ideology and profit. *Coders* are non-malicious hackers with upper-intermediate skills who seek prestige. *Criminals* have an upper-intermediate skill set and are primarily motivated by profit and secondarily by revenge. *Insiders* have middling skills and are motivated by revenge or profit. *Crowdsourcers* use less technical means and are motivated first by revenge and second by recreation. *Novices* employ basic techniques and are motivated by curiosity. *Punks* have low to average skills and are motivated primarily by the thrill of participating in deviant behavior and secondarily by revenge.

While Figure 1 is useful in presenting a general typology of hacker types, the circumplex model can also be used to categorize case studies. Figure 2 replaces the generic hacker classes of Figure 1 with representative cases, including how those cases relate to one another. In that sense, it is an amalgamation of a sociogram and a circumplex. A representative example of the relationship between hacker groups can be found in the ties between Anonymous—a loosely connected, leaderless movement of hackers—and its offshoots: LulzSec, AntiSec, and MalSec. Whereas Anonymous rose to prominence as defenders of an open Internet and freedom of speech, some of its offshoots adopted a more recreational ideology—conducting cyber attacks for self-amusement (Pendergrass, 2013). As the ideologies of these offshoots shifted, and as law enforcement agencies cracked down, these factions

disbanded or shifted towards new offshoots (Pendergrass, 2013). For instance, when the FBI arrested several hackers charged with ties to LulzSec and AntiSec—groups whose activities involved dumping usernames and passwords en masse online, thus exposing many to privacy risks—a new offshoot, MalSec, emerged declaring more altruistic goals such as exposing security flaws online without endangering civilians (Murphy, 2012). Figure 2 captures the relationship between these offshoots and their positions in the hacker typology by depicting shifts in motivation and sophistication, particularly the shift towards prestige (these offshoots were well known for publicly bragging of their exploits) and ideology, compared to the original group (Anonymous).

[Insert Figure 2 about Here]

Circumplex models can also be used to reveal enabling relationships, such as the collection of criminal marketplaces in the profit sector of Figure 2 centered on Tor, an anonymizing service that enables users to browse the Internet incognito. Here the black market networks Silk Road, Sheep Marketplace, Black Market Reloaded, and Atlantis, while not directly tied to one another, are indirectly connected in that their activities are facilitated via the Tor network (Gibbs, 2013; Hern, 2013). In this sense, akin to a two-mode network in social network analysis, this circumplex with sociogram elements portrays the relationship between the technological and social sides of cyber behavior.

Another example is found in Chinese mercenary hacking groups such as Hidden Lynx and Net Traveler. Even though no direct links have been found between these groups and the Chinese government (Finkle, 2013), evidence that attacks by these groups originate in China and are often directed at American and Taiwanese targets in the defense industry insinuates patriotic motivation or indirect approval by the Chinese government (Doherty et al, 2013). This suggests that the Chinese government may be a client of Hidden Lynx rather than its governor (Doherty et al, 2013), which would benefit the Chinese government in the sense that they could reap the profits of cyber attacks without incurring the risks, thanks to the plausible deniability of outsourcing attacks.

That circumplex models can be used to depict indirect relationship increases their usefulness in combatting cyber malfeasance by revealing the complex relationships between hackers and their enablers. In that sense, circumplex models can be paired with network data to indicate relationships between hacker groups, the computer systems they use, the locations of their targets, their methods used, and their purported motivations. Classifying cyber adversaries as such can aid the development of appropriate countermeasures by grouping threats by commonalities and informing risk management decisions (Boin and McConnell, 2007; Buyens et al, 2007; Farahmand et al, 2005; Lindqvist and Jonsson, 1997; Friedman and Hoffman, 2008).

The Weighted Arc Circumplex Model

Although the circumplex models above are useful in presenting the relationships between hacker types, capabilities, motivations, and case studies, they are limited in that they assume single or dual motivations even though many hackers are driven by multiple motivations (Rogers, 2010). Consider Figure 1, which implies that crowdsourcers are motivated by revenge and recreation. While this is generally true, many crowdsourcers are motivated by ideology as well (Wang et al, 2010), information that is lost in the modified circular order circumplex model pioneered by Rogers (2006) and adopted by Meyers et al (2009).

In that vein, I propose a weighted arc circumplex model that allows for multiple motivations to be displayed for a given hacker type¹. In this adaption, instead of plotting small nodes in a single sector, archetypes are depicted by an arc that potentially crosses multiple sectors, signaling multiple motivations. To depict the different degrees of influence among motivations, the arcs are weighted, with the thickest segment indicating a primary motivation and ever-thinning segments indicating secondary, tertiary, quaternary, or quinary motivations. The weighted arcs of the circumplex models in this paper are based on qualitative data on hacker archetypes delineated in the literature and are meant to be exemplary (see the Constructing Hacker Typologies section below). Ideally, future research could

employ more quantitatively oriented weighting techniques, but that is beyond the scope of this paper. Nevertheless, Farahmand et al (2005) believe that, even in the absence of quantitative data, qualitative analyses remain useful to securing information systems.

Figure 3 is an adaption of Figure 1, a general typology of hackers that utilizes the weighted arc format. In comparing the figures, one can see that the weighted arc circumplex offers a more versatile and more accurate depiction of hacker types. For example, the hacktivist node in Figure 1 is placed in the ideology sector, as that is the primary motivation for most hacktivists. However, the simplicity of that circumplex results in a loss of information that conceals the fact that hacktivism is a broad category of cyber activity motivated by more than ideology. In contrast, the weighted arc for hacktivists in Figure 3 reveals secondary (recreation), tertiary (prestige), and quaternary (revenge) motivations.

[Insert Figure 3 about Here]

[Insert Figure 4 about Here]

This presentation of hackers can also be applied to case studies for greater insight into the motivations behind real-world cyber adversaries. Figure 4 is an abridged version of Figure 2 that removes certain case studies, for simplicity, but expounds on others, offering a more nuanced portrayal of the relationships between hacker groups and their motivations. Illustrating this point, the Anonymous hydra in Figure 2 insinuates that Anonymous was motivated primarily by revenge, which overlooks the importance of ideology as a motivating force (Pendergrass, 2013).

This is perhaps the biggest shortcoming of previous circumplex models used to categorize cyber actors: sectors must be adjacent for a relationship to be implied. However, the complexity of cyber actors and the multitude of motivations driving their behaviors means that different groups have different overlapping motivations that cannot be captured by the circumplex models employed by previous research. In contrast, the weighted arc format is more versatile in that it can display groups with motivations in non-adjacent sectors of the circumplex, such as displaying a hacker motivated by

both recreation and prestige, which can be depicted in the weighted arc model but not in its predecessor.

This benefit is seen in how Figure 4 portrays the Anonymous hydra, in which it becomes evident that Anonymous's activity stems from an array of motivations. The weighted ends and narrow middle of the Anonymous arc suggest that revenge and ideology are the primary and secondary motivations driving their activity, with recreation and prestige as a tertiary and quaternary impetuses. This fits with the Anonymous story and provides a clearer picture of the relationship between Anonymous and its offshoots (Lulzsec, AntiSec, and MalSec), who defected because they had different primary motivations than the original group (Pendergrass, 2013). The arc of the original faction, LulzSec, captures their primary (recreation), secondary (prestige), and tertiary (ideology) motivations. Subsequent offshoots such as AntiSec and MalSec indicate further motivational shifts toward ideology, hacking in the name of a freer Internet. Finally, Wikileaks is also depicted, not because it is directly connected to Anonymous but to represent an informal connection, as Anonymous rose to prominence in their defense (Pendergrass, 2013). This is another example of how these circumplex models can be merged with social network data to depict both direct and indirect, social or technical relationships between cyber actors.

Constructing Hacker Typologies

The hacker types displayed in the circumplex models above come from a review of extant hacker typologies (Chantler, 1996; Landreth, 1985; Meyers et al, 2009; Rogers, 2006, 2010), case studies (Doherty et al, 2013; Finkle, 2013; Glenny, 2011; Holt, 2009; Pendergrass, 2013; Wang et al, 2010), newspaper articles (Gibbs, 2013; Glenny, 2013; Hern, 2013; Murphy, 2012), and original writings published by hacker groups. In short, I examined extant taxonomies, further informed them with updated information from case studies, newspaper reports, and original writings, and then qualitatively categorized them by motivation and sophistication.

As an example, regarding motivation, LulzSec self-identified as having primary recreational and secondary ideological motivations, posting links on their official Twitter account (@LulzSec) to manifestos declaring that they hack “for the laughs” as well as political ideology (Pendergrass, 2013), such as their hacking of the Arizona Department of Public Safety in opposition to SB1070, a bill granting law enforcement officers the right to ask for documentation from suspected illegal immigrants (Clayton, 2011). They were also known as braggarts, publicly boasting of successful hacks as a means of gaining media attention. I therefore coded LulzSec as a hybrid of punks and hacktivists. This is seen in Figure 4 where their motivations overlap between recreation, prestige, and ideology, with their thickest arc segment in the recreation sector, a subsequently thinner arc segment in the ideology sector, and an even thinner arc segment in the prestige sector. This is also an example of how the weighted arc circumplex (Figure 4) improves on the circular order circumplex model (Figure 2), which cannot capture these nuances.

Attack sophistication was determined by a group’s attack history and categorized according to extant scholarship (Meyers et al, 2009; Doherty et al, 2013). If a group employed fairly sophisticated techniques (e.g. SQL injections, DDoS) that damaged high status targets, they were deemed more sophisticated than hackers running pre-written scripts but less sophisticated than groups using more advanced techniques against even higher status targets. For example, LulzSec used fairly sophisticated techniques to exfiltrate sensitive data from or disrupt the networks of dozens of high profile targets (e.g. Sony, PBS, and Fox). In comparison, mercenary hackers such as Hidden Lynx simultaneously attacked higher profile targets (e.g. U.S. defense contractors), using “cutting-edge,” customized Trojans (Doherty et al, 2013:4). Thus, in relation to the other groups, LulzSec were coded as having middle-intermediate sophistication and Hidden Lynx was coded as highly sophisticated (see Figure 4). Although information about hackers is difficult to come by, aggregated information about hacker types will, over time, ever

increase the usefulness of these types of hacker typologies, particularly for typological visualizations such as the weighted arc circumplex model.

Practical Applications

Circumplex models of hackers aid cyber security as a useful investigative tool thanks to their quick visualization of threats (Rogers, 2006). As Rogers (2006:101) notes, a circumplex model is useful because it “allows investigators to benefit from the same investigative support that behavioral analysis provides to other more traditional criminal investigations.” This is because the circumplex provides “a quick visual representation of the interactive effects of the primary components” of cyber attacks (101). In contrast, continuum-based approaches only model one dimension at a time, making the interactions of the components harder to identify. Thus, circumplex models enable investigators to analyze complex threats more efficiently, and the weighted arc models proposed here are particularly suited for visualizing various cyber adversaries. As such, network administrators making risk management decisions on how to most efficiently prepare for cyber threats can benefit from the weighted arc circumplex model by quickly being able to determine how likely their organization will be a target of a certain type of hacker.

For instance, if an attack on a company originated externally, targeted only the corporate Web page, was of middling sophistication (e.g. SQL injection), and a brag screen was left behind, investigators could use the hacker typologies depicted above to winnow down the list of suspects to cyber punks. Conversely, if an attack originated externally and targeted only the financial sectors of the network, the hacker typology would alert the company that they were a target of criminals. The company can then focus their limited resources into defending against these types of attacks by these types of hackers. Alternatively, if the organization is political, it can examine the typology and prepare for attacks likely stemming from groups identified as having ideological motivations. In short, the weighted arc circumplex model can aid risk-management decisions by making clearer who is most likely to attack. This

information can then be paired with known attack techniques and proven defenses against them (see Friedman and Hoffman, 2008:170).

Weighted arc circumplex models, particularly those that incorporate social network data, can serve as a starting point for more tailored cyber security analyses. For example, Holt et al (2012) analyzed the social networks linking together various Russian hacker groups. The sociograms in their research could be paired up with accepted hacker types—and their skills and motivations—delineated here and converted into circumplex models. This is similar to the Anonymous hydra case study presented in Figure 4, which breaks out the hacktivist arc of Figure 3.

Furthermore, circumplex models can be further broken down into sub-models which delve into the complex data that compose cyber security analyses. Using this sub-modeling strategy, computer security administrators could spin out those groups with a given motivation such as ideology and then further parse out the specific ideologies that provide their unique motivations. These more detailed sub-models can, in turn, better aid the identification of potential targeted organizations and the hackers targeting them. Specifically, each of the hacker archetypes in Figure 3 could subsequently be featured in their own circumplex models that further delineates the types of groups comprising that archetype and their unique motivations. The dissection of the hacktivist archetype of Figure 3 into the more detailed examination in Figure 4 of the Anonymous hydra is an example of this, but such sub-models could also be flexible enough to consider more detailed motivations as well (e.g. the types of ideologies that comprise the ideology sector). Creating sub-models of hacker types would be one way of compensating for the biggest shortcoming of using parsimonious categorization systems: collapsing things together obfuscates their differences. Thus, as targeted organizations accumulate cyber security data, they can further customize potential threats that are most relevant to them.

Discussion

Categorizing threats is a common risk management strategy that enables administrators of complex systems to prioritize the allocation of limited resources to address the most likely threats. Mirkovic and Reiher (2004) list several benefits of categorization relevant to cyber security specialists. First, it provides a map of the field, offering a quick, comprehensive overview for novices. Second, it makes known new threats, which helps cyber security evolve just as cyber malfeasance evolves. Third, it provides a common vocabulary, which fosters cooperation among researchers and network administrators. Fourth, it facilitates efficient responses to incidents, enabling administrators to focus on subsets of threats rather than unrealistically focusing on all potential threats.

As a categorization tool, circumplex models are beneficial in compiling information about known cyber threats and presenting this information visually, thereby enabling cyber security specialists and targeted organizations to counter cyber attacks more efficiently by tailoring their strategies accordingly. This approach contrasts with the one-size-fits-all approach to cyber security that myopically lumps all hackers together, thereby wasting time and resources defending against unlikely threats.

In this essay I addressed the anachronism of existing hacker typologies by updating extant circumplex models with new types of hackers and new methods for classifying them, revealing how the field has changed over time. In fact, the evolution of classification schemes can itself provide useful information, introducing new threats and retiring old ones. A history of previous versions of a typology can be used to track which threats are new, much like how the current models in this paper can be compared to Meyers et al (2009)'s model, which can be compared to Rogers's (2006) model, and so forth, to see how cyber threats have evolved over time.

Following that, examining existing hacker typologies reveals that they do not emphasize social or ideological motivations, which, according to the Theory of Planned Behavior (TPB), are two crucial determinants of human behavior, including those of cyber actors (Gordon and Ma, 2003). This paper therefore contributes to the field of categorizing cyber malfeasance by highlighting ideology as a

primary motivation for certain hacker types, by recognizing socially driven cyber behavior such as crowdsourcing, and by demonstrating how previous visualization tools for displaying hacker typologies—mainly, modified circular order circumplex models—can be made more versatile by transforming them into weighted arc circumplex models to visualize hacker archetypes with multiple motivations or by wedding them with sociograms to depict complex relationships between hacker groups, their offshoots, the technological or network systems they utilize, and the nuances between their skill levels and motivational stimuli.

Nevertheless, both the circular order circumplex model (Figures 1 and 2) and the weighted arc circumplex model (Figures 3 and 4) have merits in categorizing cyber adversaries. Whereas the former type provides a parsimonious presentation, the more nuanced depictions of the latter type offer more insight into relationships between hackers, their capabilities, and the motivations behind their activities. Both types of circumplex models economically display the different hacker types and their motivations, which enables researchers to profile hackers and predict future threats (Fitch, 2003). However, the weighted arc circumplex model proposed in this paper offers the ability to more thoroughly and accurately depict hacker types with multiple motivations.

That said, determining hackers' motivations is not an easy task since many hackers prefer discreetness to notoriety, but one way to do so is to identify their targets (Doherty et al, 2013). Consider that attacks against financial institutions are likely to be motivated by those seeking financial gain. As hackers tend to attack similar targets using similar strategies, using targets to identify motivations, and consequently to categorize hackers, enables targeted organizations to prepare for certain types of attacks (e.g. phishing or social engineering attacks on financial employees), which will lower the costs and improve the efficiency of cyber defense systems. Importantly, though, one must use caution when using this approach as it is not always an accurate assumption, as hackers motivated by ideology, recreation, revenge or profit might attack the same site (e.g. the Pentagon) but for different reasons. Of

course, high status targets like federal institutions or major corporations need to be prepared for all types of cyber attacks, making the circumplex models described in this paper less useful to these types of targets. Instead, employing such models would most benefit small businesses and organizations with limited resources for cyber defense that are niche targets, such as local credit unions (likely targets from criminals) or local political organizations or campaigns (likely targets of hacktivists or punks).

This limitation is also an opportunity in interdisciplinary collaboration, such as wedding sociological theories of online deviance with psychological (e.g. Fitch, 2004; Fotinger and Ziegler, 2004; Seigfried-Spellar and Treadway, 2014) or criminological (e.g. Holt et al, 2012; Marcum et al, 2014; Steinmetz, 2015) theories on hacking, which could further increase the accuracy and usefulness of hacker typologies by testing their robustness or suggesting alternative parameters for classification. For instance, Seigfried-Spellar and Treadway (2014) found that personality traits influence who hacks and who does not, as well as the types of hacking one partakes in, whereas Marcum et al (2014) drew on General Theory of Crime and Social Learning Theory to show that low self-control and deviant peer association were related to hacking by juveniles.

Nevertheless, any type of taxonomy or typology is limited in that they condense complex entities (Rogers, 2010). The weighted arc circumplex models in this paper seek to mitigate that concern by allowing the depiction of multiple motivations for a given archetype, but, as with any categorization scheme, the benefits of parsimony come at the expense of detail: collapsing any group of individuals into categories always results in information loss, which may be problematic when categorizing cyber deviants, who have been shown to engage in multiple types of cyber malfeasance rather than mutually exclusive categories (McBrayer, 2014). Recall that the circumplex models used by Rogers (2006, 2010) and Meyers et al (2009) employed four overarching motivations whereas the models in this paper add a fifth motivation. Unsurprisingly, other studies that categorize hackers feature different types and numbers of motivations (e.g. Chantler, 1996; Landredth, 1985; McBrayer, 2014, Taylor, 1999). Given this

lack of consensus on hacker motivations, as well as the dynamism of contemporary cyber malfeasance, further research in a variety of fields such as sociology, psychology, and criminology is needed to continually refine hacker typologies.

Ultimately, investigators must consider as many parameters as available, only making hard classifications when there is substantial evidence to do so, for allocating limited resources based on hastily categorized threats may result in network security holes. When used appropriately, though, hacker typologies are a useful tool for combating threats to critical infrastructure such as internets and intranets (Rege-Patwardhan, 2009).

Acknowledgements

* This paper has been supported by National Science Foundation Grant No. [temporarily redacted by the author to preserve an anonymous peer-review process]. I thank [temporarily redacted by the author to preserve an anonymous peer-review process] for their comments on earlier versions of this paper.

Endnotes

1. Technically, it is a modified circular order, weighted arc circumplex model.

Works Cited

- Bailey, Kenneth D. 1994. *Typologies and Taxonomies: An Introduction to Classification Techniques*. Thousand Oaks, CA: Sage.
- Boin, Arjen and Allan McConnell. 2007. "Preparing for Critical Infrastructure Breakdowns: The Limits of Crisis Management and the Need for Resilience." *Journal of Contingencies and Crisis Management* 15(1):50-59.
- Buyens, Koen, Bart De Win, and Wouter Joosen. 2007. "Empirical and Statistical Analysis of Risk Analysis-Driven Techniques for Threat Management." *IEEE Computer Society, The First International Workshop on Secure Software Engineering*, Vienna, Austria, April 10-13. Accessed on 9 April 2015 (<https://lirias.kuleuven.be/bitstream/123456789/146252/1/paper.pdf>)
- Chantler, Nicholas. 1996. *Profile of a Computer Hacker*. Florida: Infowar
- Clayton, Mark. 2011. "What does LulzSec Want? Hack of Arizona computers Offers Clues." *Christian Science Monitor*, 24 June.
- Doherty, Stephen, Jozsef Gegeny, Branko Spasojevic, and Jonell Baltazar. 2013. "Hidden Lynx: Professional Hackers for Hire." *Security Response*, Symantec Corporation. Accessed on October 22, 2013 (http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/hidden_lynx.pdf).
- Egan, Matt. 2011. "Hackers with a Conscience? Ideological Attacks Complicate Cyber Defense." *Fox Business*, 15 December. Accessed on 27 February, 2014 (<http://www.foxbusiness.com/technology/2011/12/15/hackers-with-conscience-ideologically-motivated-attacks-complicates-cyber/>)
- Farahmand, Fariborz, Gunter P. Sharp, and Philip H. Enslow. 2005. "A Management Perspective on Risk of Security Threats to Information Systems." *Information Technology and Management* 6:203–225.
- Finkle, Jim. 2013. "Hacker Group Found in China, Linked to Big Cyberattacks: Symantec." *Reuters*, 17 September. Accessed on October 22, 2013 (<http://www.nbcnews.com/technology/hacker-group-found-china-linked-big-cyberattacks-symantec-4B11180871>).
- Fitch, Cynthia, 2004. "Crime and Punishment: The Psychology of Hacking in the New Millennium". *Bethesda, MD: SANS Institute*. Accessed on 9 April 2015 (<http://www.giac.org/paper/gsec/3560/crime-punishment-psychology-hacking-millennium/105795>).
- Fotinger, Christian S. and Wolfgang Zeigler. 2004. *Understanding a Hacker's Mind—A Psychological Insight into the Hijacking of Identities*. Krems, Austria: Danube University.
- Friedman, Jon and Daniel v. Hoffman. 2008. "Protecting Data on Mobile Devices: A Taxonomy of Security Threats to Mobile Computing and Review of Applicable Defenses." *Information Knowledge Systems Management* 7:159-180.

- Gibbs, Samuel. 2013. "Silk Road Underground Market Closed—But Others Will Replace It?" *The Guardian*, 3 October. Accessed on October 22, 2013 (<http://www.theguardian.com/technology/2013/oct/03/silk-road-underground-market-closed-bitcoin>).
- Glenny, Misha. 2011. *Dark Market: How Hackers Became the New Mafia*. New York: Vintage.
- . 2013. "Cyber Subterfuge." *New York Times*, 27 November. Accessed on December 1, 2013 (http://www.nytimes.com/2013/11/28/opinion/cyber-subterfuge.html?pagewanted=1&tntemail0=y&_r=0&emc=edit_tnt_20131201).
- Gordon, Sarah and Qingxiong Ma. 2003. *Convergence of Virus Writers and Hackers: Fact or Fantasy?* Cupertino, CA: Symantec Corporation
- Hern, Alex. 2013. "Silk Road Replacement Black Market Reloaded Briefly Closed." *The Guardian*, 18 October. Accessed on October 22, 2013 (<http://www.theguardian.com/technology/2013/oct/18/silk-road-black-market-reloaded-closed>).
- Hollinger, Richard C. 1988. "Computer Hackers follow a Guttman-like Progression." *Sociology and Social Research* 72:199-200. Accessed on October 22, 2013 (<http://www.phrack.com/issues.html?issue=22&id=7>).
- Holt, Thomas J. 2009. "The Attack Dynamics of Political and Religiously Motivated Hackers." Proceedings of the Cyber Infrastructure Protection Conference, City University of New York. June 4-5. Accessed on December 6, 2013 (<http://www.arifyildirim.com/ilt510/thomas.holt.pdf>).
- Holt, Thomas J., Deborah Strumsky, Olga Smirnova, and Max Kilger. 2012. "Examining the Social Networks of Malware Writers and Hackers." *International Journal of Cyber Criminology* 6(1):891-903.
- Ki-moon, Ban. 2013. "Secretary-General's Video-Message for Model UN Security Council Conference on Cyber Security." *United Nations*, 21 October, Baku Azerbaijan. Accessed on 9 April 2015 (<http://www.un.org/sg/statements/index.asp?nid=7216>).
- Landreth, Bill. 1985. *Out of the Inner Circle: A Hacker's Guide to Computer Security*. Microsoft Press.
- Lawson, Loraine. 2001. "You Say Cracker; I Say Hacker: A Hacking Lexicon." *Tech Republic*, 13 April. Accessed on October 22, 2013 (<http://www.techrepublic.com/article/you-say-cracker-i-say-hacker-a-hacking-lexicon/>).
- Lindqvist, Ulf and Erland Jonsson. 1997. "How to Systematically Classify Computer Security Intrusions." *IEEE Symposium on Security and Privacy*, Proceedings(1081-601):154-163. Accessed on 9 April 2015 (<http://ranger.uta.edu/~dliu/courses/cse6392-ids-spring2007/papers/SP97-IntrusionClassification.pdf>).
- Marcum, Catherine D., George E. Higgins, Melissa L. Ricketts, and Scott E. Wolfe. 2014. "Hacking in High School: Cybercrime Perpetration by Juveniles." *Deviant Behavior* 35(7): 581-591.

- McBrayer, John. 2014. "Exploiting the Digital Frontier: Hacker Typology and Motivation." *University of Alabama*, Thesis 1561364. Accessed on 12 May 2015 (<http://gradworks.umi.com/15/61/1561364.html>).
- Meyers, Carol, Sara Powers, and Daniel Faissol. 2009. "Taxonomies of Cyber Adversaries and Attacks: A Survey of Incidents and Approaches." Technical Report LLNL-TR-419041, Lawrence Livermore National Laboratory. Accessed on October 22, 2013 (<https://www-eng.llnl.gov/pdfs/taxonomies.pdf>).
- Mirkovic, Jelena and Peter Reiher. 2004. "A Taxonomy of DDoS Attack and DDoS Defense Mechanisms." *ACM SIGCOMM Computer Communication Review* 34(2):39-53.
- Murphy, Samantha. 2012. "Leak it for the People." *New Scientist* 214(2861):22.
- Nikitina, Svetlana. 2012. "Hackers as Tricksters of the Digital Age: Creativity in Hacker Culture." *The Journal of Popular Culture* 45(1):133-152.
- Rege-Patwardhan, Aunshul. 2009. "Cybercrimes Against Critical Infrastructures: A Study of Online Criminal Organization and Techniques." *Criminal Justice Studies* 22(3):261-271.
- Obama, Barack. 2013. "Executive Order 13636—Improving Critical Infrastructure Cybersecurity." *Federal Register*, 19 February. Accessed on 20 March 2014 <<https://www.hsdl.org/?view&did=731040>>.
- . 2015a. "Executive Order 13691 - Promoting Private Sector Cybersecurity Information Sharing." *Federal Register*. 13 February. Accessed on 10 April 2015 (<https://www.federalregister.gov/articles/2015/02/20/2015-03714/promoting-private-sector-cybersecurity-information-sharing>).
- . 2015b. "Executive Order 13694 - Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities." *Federal Register*. 1 April. Accessed on 10 April 2015 (<https://www.federalregister.gov/articles/2015/04/02/2015-07788/blocking-the-property-of-certain-persons-engaging-in-significant-malicious-cyber-enabled-activities>).
- Pendergrass, William S. 2013. "What is Anonymous?: A Case Study of an Information Systems Hacker Activist Collective Movement." Robert Morris University, Ann Arbor.
- Perrow, Charles. 1999. *Normal Accidents: Living with High-Risk Technologies*, 2nd Edition, Princeton, NJ: Princeton University Press.
- Rogers, Marcus K. 2006. "A Two-dimensional Circumplex Approach to the Development of a Hacker Taxonomy." *Digital Investigation* 3(2):97-102.
- . 2010. "The Psyche of Cybercriminals: A Psycho-Social Perspective". Pp. 217-235 in *Cybercrimes: A Multidisciplinary Analysis*, edited by Sumit Ghosh and Elliot Turrini. Springer.
- Seigfried-Spellar, Kathryn C. and Kellin N. Treadway. 2014. "Differentiating Hackers, Identity Thieves, Cyberbullies, and Virus Writers by College Major and Individual Differences." *Deviant Behavior* 35(10):782-803.

- Smith, Kevin B. 2002. "Typologies, Taxonomies, and the Benefits of Policy Classification." *Policy Studies Journal* 30(3):379-395.
- Sokal, Robert R. and Peter H. A. Sneath. 1964. *Principles of Numerical Taxonomy*. San Francisco: W. H. Freeman.
- Steinmetz, Kevin F. 2015. "Craft(y)ness: An Ethnographic Study of Hacking." *British Journal of Criminology* 55(1):125-145.
- Taylor, Paul. 1999. *Hackers: Crime in the Digital Sublime*. London: Routledge.
- Tehan, Rita. 2013. "Cybersecurity: Authoritative Reports and Resources." *Congressional Research Service* 25 October. Accessed on December 5, 2013 (<http://www.fas.org/sgp/crs/misc/R42507.pdf>)
- Turner, Barry A. 1978. *Man-Made Disasters*. London: Wykeham.
- Vegh, Sandor. 2003. "Classifying Forms of Online Activism: The Case of Cyberprotests against the World Bank." Pp. 71-95 in *Cyberactivism: Online Activism in Theory and Practice*, edited by Martha McCaughey and Michael D. Ayers. NY: Routledge.
- Wang, Fei-Yue, Daniel Zeng, James A. Hendler, Qingpeng Zhang, Zhuo Feng, Yanqing Gao, Hui Want, and Guanpi Lai. 2010. "A Study of the Human Flesh Search Engine: Crowd-powered Expansion of Online Knowledge." *Computer* 43(8):45-53. Accessed on October 22, 2013 (http://www.u.arizona.edu/~qpzhang/paper/HFS_Computer_2010.pdf).
- Wilshusen, Gregory C. 2011. "Cybersecurity: Continued Attention Needed to Protect Our Nation's Critical Infrastructure and Federal Information Systems." *United States Government Accountability Office*, March 16. Accessed on December 5, 2013 (<http://www.gao.gov/assets/130/125786.pdf>)

Figure 1 – A Circular Order Circumplex of Hacker Types

Notes: Nodes depict hacker types; nodes placed nearer to circle edges are more sophisticated; regular text indicates hacker groups; parenthesized text indicates motivations.

Figure 2 – A Circular Order Circumplex of Hacker Case Studies

Notes: Solid lines indicate a direct relationship; dotted lines indicate enabling relationships; underlined text indicates enabling entities; notes from Figure 1 still apply.

Figure 3 – A Weighted Arc Circumplex of Hacker Types

Notes: Thick arc segments indicate primary motivations; correspondingly thinner arc segments indicate secondary, tertiary, or quaternary motivations; notes from Figure 1 still apply.

Figure 4 – A Weighted Arc Circumplex of Hacker Case Studies

Notes: Patterned arcs indicate a parent group. Solid lines connect offshoots; notes from previous figures still apply.