Digital Investigation 14 (2015) 36–45

Contents lists available at ScienceDirect

Digital Investigation

journal homepage: www.elsevier.com/locate/diin

A typology of hackers: Classifying cyber malfeasance using a weighted arc circumplex model

Ryan Seebruck*

University of Arizona, School of Sociology, United States

ARTICLE INFO

Article history:
Received 5 January 2015
Received in revised form 1 June 2015
Accepted 8 July 2015
Available online 24 July 2015

Keywords:
Digital forensics
Hackers
Cyber crime
Circumplex
Typology
Taxonomy
Sociogram

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 the 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 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.

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,

* Tel.: +1 520 621 1504.
E-mail address: seebruck@email.arizona.edu.

http://dx.doi.org/10.1016/j.diin.2015.07.002

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 et al., 2007; Farahmand et al., 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 et al., 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 developer “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