CHAPTER 7

BLACK-HAT HACKERS' CRISIS INFORMATION PROCESSING IN THE DARKNET: A CASE STUDY OF CYBER UNDERGROUND MARKET SHUTDOWNS

K. Hazel Kwon and Jana Shakarian

ABSTRACT

This chapter explores collective information processing among black-hat hackers during their crises events. The chapter presents a preliminary study on one of Tor-based darknet market forums, during the shutdowns of two cryptomarkets. Content and network analysis of forum conversations showed that black-hat users mostly engaged with rational information processing and were adept at reaching collective solutions by sharing security advices, new market information, and alternative routes for economic activities. At the same time, the study also found that anti-social and distrustful interactions were aggravated during the marketplace shutdowns. Communication network analysis showed that not all members were affected by the crisis events, alluding to a fragmented network structure of black-hat markets. The chapter concludes that, while darknet forums may constitute resilient, solution-oriented users, market crises potentially make the community vulnerable by engendering internal distrust.

Keywords: Darknet; cybercrime; hidden organization; crisis; collective problem solving; virtual organization; cyber security

Networks, Hacking, and Media – CITAMS@30: Now and Then and Tomorrow
Studies in Media and Communications, Volume 17, 113–135

ISSN: 2050-2060/doi:10.1108/S2050-206020180000017007

INTRODUCTION

Internet anonymity has been an important technological attribute that allows users to shy away from government surveillance. On a positive note, anonymous activists have galvanized democratic social changes, freedom of speech, and decentralized markets, reifying the idea of "independence of cyberspace" advocated by cyberlibertarians two decades ago (Barlow, 1996, n.p.). In parallel with such democratic potentials, however, anonymity has also contributed to the increase in illicit user activities – so-called "black-hat" activities. Whereas some scholars may consider black-hat hacker activities as a form of "activism" (e.g., Maddox, Barrett, & Allen, 2016), other scholars define them as cyber-adversaries who exploit online anonymity (e.g., Fachkha, Bou-Harb, & Debbabi, 2015; Marin, Diab, & Shakarian, 2016; Robertson et al., 2017).

Whether viewed as libertarians or as adversaries, a consensus is that black-hat activities have widespread ramifications for society (Lee, 2015). According to a recent report by Symantec (2017), more than 7.1 billion personal identities, including multiple identity data for a single user, have been breached in the past eight years; spear-phishing alone has caused more than $3 billion of financial losses in the past three years; and email malware rate has jumped, from 1 in 220 emails in 2015, to 1 in 131 emails in 2016. Another report on AlphaBay, a cryptomarket that law enforcement recently seized, indicates that the market earned $600,000–$800,000 a day in revenue from "more than 250,000 listings for illegal drugs and toxic chemicals and over 100,000 listings for other things including stolen identification documents and hacking tools" (Larson, 2017, n.p.).

This chapter conducts a case study of a black-hat forum hosted in darknet. Whereas much literature on darknet has centered around technical understanding of its cyber-infrastructure (e.g., Chen, 2011) and criminological implications (e.g., Holt, 2007; Holt & Lampke 2010; Holt, Strumsky, Smirnova, & Kilger, 2012), the current study intends to examine a black-hat community from a communicative perspective, particularly focusing on ways in which users collectively handle their own moments of *crisis*. Crisis is a situation that "threatens the high priority goals of the organization and restricts the amount of time available for response" (Milburn, Schuler, & Watman, 1983, p. 1143). Almost every organization or community encounters its own moments of crises at least once in their organizational lifetime. If the members successfully overcome the crisis moment, the organization should survive and even transform the crisis into an opportunity of growth. If they fail to reach solutions, however, members may lose resources, or worst, the collective entity may become no longer sustainable. Black-hat communities are no exception.

This study intends to advance knowledge on how black-hat hackers gather "community intelligence" to cope with uncertainties and anxieties during their crisis moments (Oh, Agrawal, & Rao, 2013, p. 408). As Mahmood, Siponen, Straub, Rao, and Raghu (2010) point out, black-hat research "would be a breath of fresh air" for information system and online community scholarship, which has been based on mostly "white-" or "gray-hat" research (p. 432). Specifically, we analyze user conversations in one of Tor-hosted forums dedicated

to cryptomarket information sharing. A market shutdown is one of the most detrimental crisis events for black-hat users because it incurs not only monetary losses but also physical arrests by law enforcement.

In the following section, we define a darknet black-hat community as a hidden organization, and introduce a theory-driven analytic framework that we refer to as Crisis Information Processing in Hidden Organizations (CIPHO). We then introduce our case study by describing the community and crisis events of interest. The results section presents content and network analysis based on the CIPHO framework, followed by the discussion section.

BACKGROUND

Darknet Black-Hat Community as a Hidden Organization

Darknet refers to a set of hidden services in crypto-networks accessible only through particular protocols. Perhaps the most popular crypto-network today is known as Tor (The Onion Routing), which utilizes globally spread nodes through which the user is looped before accessing the website of choice. Although Tor can be used to access Surface-web sites – a sites hosted in World Wide Web, also known as "clearnet" sites (if they are not blocking Tor exit nodes), Tor-hosted sites can only be reached with the Tor-browser. Another software that allows the access to darknet is Invisible Internet Project (I2P, also known as Garlic Routing), although it is a less popular tool than Tor.

Research on the darknet has taken various computational approaches to understand technical and infrastructural aspects of the system. For example, studies have examined topological properties of inter-site dark networks (Ionită & Patriciu, 2014; Xu, Chen, Zhou, & Qin, 2006); used community detection algorithms to identify clusters of online extremist and hate group networks (Zhou, Reid, Qin, Chen, & Lai, 2005); and analyzed cybercriminal Internet Chat Relay networks (Décary-Hétu & Dupont, 2012). Also, computational methods such as topic modeling, network analysis, UserRank algorithms have allowed researchers to identify key players in the darknet forums (Décary-Hétu & Dupont, 2012; L'Huillier, Rios, Alvarez, & Aguilera, 2010; Marin, Shakarian, & Shakarian, 2018; Yang, Tang, & Thuraisingham, 2010). Researchers have also developed data mining techniques to retrieve various sources of "dark data" such as emails, instant messages, online forums, chatrooms, and cryptomarkets (Abbasi & Chen, 2007; Benjamin, Holt, & Chen, 2015; Ionită & Patriciu, 2016). Other studies have given insights into behavioral patterns of black-hat users across multiple disjointed cryptomarkets (Marin et al., 2016; Robertson et al., 2017).

Whereas computer and information science literature has remarkably advanced infrastructural understanding of darknet, these studies are primarily motivated by cybersecurity goals and thus tend to view the darknet as a malefactors' haven. In contrast, ethnographic and cultural studies often approach their cases with a libertarian view, sometimes unwittingly overemphasizing the cultural liberalism of the darknet, as alluded to by various monikers ranging from "quirky programmers"

(Nissenbaum, 2004) to "craftsmen" (Steinmetz, 2015), to "political subversives" (Coleman, 2014), and to "constructive activism" (Maddox, Barrat, Allen, & Lenton, 2016). As such competing images of darknet suggest, understanding the human side of black-hat hackers requires to consider their dual "faces," both as outlaws and as personal freedom seekers.

Therefore, rather than taking a dichotomous view, we examine a black-hat community by defining it as a "hidden collective" (Scott, 2013, p. 209). A hidden collective is characterized by their caution to control organizational visibility, relevant audiences, and member identifications (Scott, 2013). For example, cryptomarket-based communities need to attract more vendors and consumers for profitability. Simultaneously, however, increasing the community's visibility to careless users and novices could endanger the security of community (organizational visibility). As a result, these communities promote their visibility more restrictively than conventional online communities, often imposing a selective entry barrier to eliminate risky audiences, for example, using a referral system (relevant audiences). Furthermore, total anonymity is regarded as the most loyal way for a member to show dedication to the community. Therefore, even members within the same community conceal their identities from one another.

In other words, minimal visibility, selective promotion, and invisible loyal members are the essential features of hidden collectives including black-hat communities in darknet. To our knowledge, little research has explored how such hiddenness and exclusivity influence the crisis management processes of black-hat hacker communities in particular, and hidden organizations in general. On the one hand, a crisis could make hidden organizations even more vulnerable to destabilization than "normal" organizations because being anonymous even among peer members could intensify uncertainty and thus trigger distrust spread within the community. On the other hand, hidden organizations could function more effectively than "normal" organizations to cope with the crisis: The secrecy and exclusivity could solidify members' shared identity that promotes collective actions. By examining the crisis information processing in the black-hat community, we discuss how members of a hidden organization respond to a crisis event.

Crisis Information Processing in Darknet Communities

Systematic understanding of crisis management in black-hat communities (and other hidden organizations) begs for a theory-driven analytical framework. We introduce a framework referred to as *CIPHO*. This framework highlights three theoretical concepts.

Crisis. A crisis is characterized "by high consequence, low probability, ambiguity, and decision-making time pressure" (Runyan, 2006, p. 13). These characteristics induce anxiety and uncertainty, which in turn create the need for communication among the affected members (Allport & Postman, 1947). Considering that anxiety and uncertainty are known as universal emotional and cognitive reactions to crisis (Allport & Postman, 1947; Oh, Kwon, & Rao, 2010), we expect these reactions should be observed in black-hat communities as well. That is, CIPHO should address the affective and cognitive needs as triggers for further collective information processing.

Collective problem solving. We take "*groups* as information processors" theory as a baseline of CIPHO (Scholten, van Knippenberg, Nijstad, & De Dreu, 2007, p. 22). The group information processing literature has fallen in line with the classical task-oriented view that centers on rational decision making (Galbraith, 1974). As mentioned earlier, however, crisis situation is differentiated from a regular problem-solving situation because in crises group members collectively undergo not only cognitive uncertainty but also emotional unrest (e.g., anxiety, fear). Accordingly, another dimension of information processing, pertinent to emotion and intuition-driven problem solving, could become as prominent as rational information processing. Previous research has defined such non-rational information processing as "experiential" processing, and found that experiential processing is orthogonal to rational processing: it runs independently from rational processing, and thus can occur simultaneously with rational processing (Epstein, 1994; Stark, Baldwin, Hertel, & Rothman, 2017).

Black-hat hackers in darknet are highly rational and instrumental actors in ordinary times (Moeller, Munksgaard, & Demant, 2017). It is unknown, however, whether their rational choice tendency would remain as a dominant problem-solving mechanism during crisis. Considering the potential role of intuitive information processing during crisis, CIPHO incorporates both rational and experiential information processing into the framework.

Anonymity. Anonymity is an essential feature of hidden collectives, including darknet communities. Anonymity amplifies social processes in both pro- and anti-social ways. On a positive note, the absence of individuating markers highlights collectively shared identity, which in turn reinforce pro-community interactions (Lee, 2007; Postmes, Spears, & Lea, 1998). Conversely, however, anonymity can also encourage disinhibited behaviors such as offensive interactions, trolling, or hate speech (Cho & Kwon, 2015; Herring, Job-Sluder, Scheckler, & Barab, 2002; Moor, Heuvelman, & Verleur, 2010; Suler, 2004). Anonymity not only influences the ways in which black-hat users interact with one another but also is the most important condition to survive as a group. Considering the importance of anonymity in sustaining darknet black-hat communities, we add two elements to CIPHO: anonymity-based social processing as a part of collective problem-solving processes, and identity concealment as a crisis coping strategy.

Based on the discussions above, CIPHO proposes a three-dimensional framework, which includes (a) needs for information processing; (b) information processing for collective problem solving, composed of rational, experiential, and anonymous social processes; and (c) steering crisis-coping strategies, including how to maintain anonymity. Each conceptual dimension consists of sub-categories of "communication acts" that are operationalized for content analysis: *anxiety* and *uncertainty* for the needs for information processing; *personal narrative* and *reliance on source credibility* for experiential collective information processing; *information providing* and *deliberation* for rational collective information processing; *pro-community* and *anti-social messages* for anonymous social processing; and *procedural directives* and *identity concealment strategies* for crisis-coping. Although these categories were drawn from various information processing literature, a large part of the CIPHO framework was inspired by Rumor Interaction Analysis System (RIAS), one of the few models

designed to study group interactions in online communities (Bordia & DiFonzo, 2004; Oh et al., 2010). Whereas RIAS pertained exclusively to rumor communication, the utility of CIPHO is to examine hidden organizations' crisis communication, with an emphasis on the role of anonymity. The descriptions and exemplary messages for the communication categories are summarized in Table 1. Based on the CIPHO framework we ask the following questions:

RQ1. What types of "communication acts" were the most salient in the darknet black-hat community under crisis events?

RQ2. How was communication network in the black-hat community configured based on the CIPHO framework?

DATA: CASE STUDY

The Study Site: The Forum "W"

Founded in 2011, the "W" is a Tor-based community dedicated to cross-marketplaces affairs and news sharing. It uses English language and is one of the few communities that allow users to exchange information about different crypto-marketplaces in one place without the need to visit a specific market forum separately. At the time of writing it boasted of 36 discussion boards, comprising nearly 41,000 registered users, who contributed to about 135,000 posts (lifetime). Like most online forums, the "W" is composed of multiple discussion boards and threads. The platform is long standing and still enjoys everyday activity by a multitude of darknet users throughout its boards. In fact, the most active period of its lifetime measured in the highest number of users online simultaneously was very recently, in mid-October 2017.[1] The ways in which this forum is organized and operated are similar to the conventional, visible online communities as described below (see Appendix for the annotation of darknet terminologies).

Registration and Rules

The prospective member should agree to the rules of the platform to register. Direct trade, child pornography, fraud, weapons, and explosives are prohibited as is doxing (the exposure of personally identifiable information of individuals). Although the forum dedicates much content to marketplaces and vendors, it bars advertisements of products and services. Like other online communities, spamming and trolling are not tolerated. Aside from choosing username and password, prospective members should provide with an email address, with the option of whether other users may contact them via email. Email confirmation is not triggered. The final step of the registration prevents automated scripts from accessing the site by positing CAPTCHA in addition to one out of a limited set of questions (e.g., "How many months are in a year minus X" or "How many days in the week not counting Y").

Table 1. Crisis Information Processing in Hidden Organization (CIPHO) Framework.

Conceptual Dimension	Communication Types	Definition
Needs for information processing	Anxiety	Displaying fear, anxiety, frustration, etc. "pretty scary," "this isn't looking good there are a lot of unhappy customers here"
	Uncertainty	Seeking information, or hesitance due to the lack of information "can you explain what you mean by vacation mode?" "been trying to sign up for 3 days but keep getting registration failed? Help?"
Experiential processing	Source credibility	Adding credibility by referring to external sources or experts, or by claiming their own expertise "we have some news http://…," "according to someone on reddit…" "police has confirmed that they've seized the market site"
	Personal narrative	Personal experience or involvement to a situation "I've been placing orders for months on pandora by now, and have not run into a single problem!" "all my vendors have removed listing and have moved on. I am still hanging around because I would like to get my money back"
Anonymous social processing	Pro-community	Community supportive, amicable message, or an expression of solidarity "interesting post, thanks for sharing," "the universe will not let le (law enforcement) ever catch you for you service. respect"
	Anti-social/ disinhibition	Ridiculing, attacking, offensive commenting, trolling "gimme that 0.1 you whore!" "a big fuck you to the mods who are all pigs. doctorclu in particular is like squealer in addition to being a dog"
Rational processing	Information providing	Fact or fact-like statement "sharedsend has been replaced with an open source solution called sharedcoin," "no auto withdraw at bsm anymore," "uk lbc has stopped withdrawals"
	Deliberation	Analyzing; disputing; agreeing/disagreeing with; drawing inferences from what someone else had said; elaborating one's own views, actions, and beliefs "I don't think a market wants to store all those signed keys nor does a vendor want to go thru the burden of creating them all." "after looking at some interesting sr1 forum posts and doing some discreet googling, the grand wizard may not know exactly who was responsible for the sr2 scam"
Crisis coping	Concealment strategies (i.e., OpSec)	Actionable items that respond to troubles-hooting, or technical solutions for concealment "to do this:go to profile > account settings > then uncheck the option that shows people you are online," "pgp does not have to be a pain to use. the easiest pgp program to use for windows and linux users is gpg4usb which you can download at this clearnet link: http://"
	Procedural directives	Moderating or facilitating discussion within the community "please avoid double posting it only slows us," "please update this thread"

The same precautions are taken before submitting a post anywhere on the site. A newcomer should contribute 20 posts in the beginner section before adding to other sections, although the entire forum content can be viewed. Specifically, there are threads for new members to introduce themselves and reiterations of rules and regulations.

Social Structure

Founders, administrator, and master contributors are highest ranking in the hierarchy of the forum. At the time of writing, the administrator had authored over 700 posts. Peer ratings are common throughout forums dedicated to all manners of content. The signature displayed like a footer after each posted message encourages donations to the forum, although no transactions or balance are logged for the given address on the blockchain. Below the rank of the administrator, moderators are responsible for maintaining the integrity of the content within their assigned board. The boards also feature "global moderators" who appear to be long-standing members as it appears that their total number of posts often exceed even that of the administrator(s). However, reputation as indicated by the community ranking is not coinciding with the number of posts. Moreover, the functionary ranks of administrator or moderator are parallel to and independent from ranks earned by frequency of activity (total number of posts) in this forum. New members and less active contributors form the majority and lowest ranks of the membership.

Anonymity and Operational Security (OpSec)

For vendors and buyers alike darknet markets constitute considerable risks as well as benefits. Discussions about market features, admins as well as the vendors and products featured seek to gauge the site's reliability. Any signs of transaction frauds and lackadaisical responses toward alleged fraud arise immediate suspicion. Increased frequency in the sites' unavailability is frowned upon as it may foreshadow imminent permanent closure. The Tor-browser allows users to block JavaScript which allows finger-printing – "leaking" information on configurations as well as browsing behavior. Whenever a site dedicated to malicious hacking requires JavaScript to be enabled, presumably for optimal functionality, it is quickly regarded as a "honeypot." Users suspect the site has been hijacked by law enforcement, which now is trying to track and identify visitors.

On many of these sites and even a standard item on general-use Tor-directories, extensive content space is dedicated to OpSec – or "How to stay anonymous (and safe) on Tor." Virtual reams of tutorials inform on best practices, URLs to obtain and review additional anonymity measures (such as VPNs, Tails, and PGP-Keys), and topics of conversation always to be avoided.

Market Information

The "General Discussion" board in this forum encourages content on cryptocurrencies, featured (recommended) vendors and vendor reviews. Because the site appears to favor drug trade, information on safe (stealthy) shipping methods,

drug safety, and legal advice can be found. A separate board is dedicated to marketplaces: it introduces new markets, reviews prominent underground markets, and updates a list of defunct markets. Another board, an off-topic section, offers space to capture all the content not wanted in the organized boards. This aids the moderators in keeping the content on the more valued boards focused. A notable sub-board under the off-topic section board provides banned members with an outlet, although it is explicated that nothing they post would restore their accounts' legitimacy. Most other platforms do not bother retaining transgressors. It is possible that this sub-board provides proof of policing to deter other members from breaking community rules. It also serves as a space for entertainment in a forum that otherwise seeks to focus on stern and serious matters.

Pseudonymity

Avatars, bylines, and signatures can be added to allow forum members to create their own personas in the forum. References to popular media and historical figures, especially underdogs and characters with an ambivalent image are prevalent (e.g., Nero, Fox Mulder, Azrael, Cthulhu). However, some users chose names more closely aligned with their intent and include references to products (i.e., drugs) and markets. The ambience is casual, even displaying joking relationships in most parts and turns to outright silliness and trolling in the section frequented by banned members. Contributions are rated according to their usefulness, although negative votes appear to be applied for unmeasured, unmannered posts – not necessarily or solely for unhelpfulness. Higher reputation tends to encourage greater readership and more responses than contributions by users of lesser reputation. In such a social structure, establishing a good reputation is arduous and takes time. But once a good standing is attained, further improvements to social standing come more fluently.

THE CRISIS CONTEXTS: CRYPTOMARKET SHUTDOWNS

As a case study, we explored the ways in which members on "W" interact with one another facing market shutdowns. A shutdown of a cryptomarket could be one of the more damaging crisis events in the darknet. Marketplaces can be compromised either permanently or temporarily due to various reasons such as the seizure by authority, technical errors, hacking/theft by other darknet-members, or exit-scams (Moeller et al., 2017). The cases we explored trace back to February 2014 when two markets were coincidently shut down one after another. These two marketplaces were "Utopia" and "Silk Road 2." Both markets were hosted in Tor, with drugs constituting the main transaction items (Fig. 1).

Utopia was launched on February 3, 2014. However, it turned out to be one of the most short-lived darknet marketplaces. A week after opening, on February 11, 2014, Dutch police seized Utopia, along with the onsite-stored bitcoins

Fig. 1. Screenshot of Utopia Homepage (Left) and Silk Road 2 Homepage (Right). Adapted from deepdotweb.com.

amounting to $610,900. The police also arrested five suspects (four Dutch; one German) who allegedly ran the market (Deepdotweb, 2014).

Silk Road 2 (SR2) was opened on November 3, 2013. While the original owners of SR2 were arrested in December, 2013, the marketplace continued, operated by a temporary administrator using the pseudonym "Defcon." Subsequently SR2 was hacked and temporarily shut down on February 13, 2014. The compromise of the marketplace resulted in the loss of bitcoins equivalent to $2.7 million dollars (Deepdotweb, 2014). On February 18, 2014, the alleged hackers of SR2 were doxed. Afterwards, the market reopened and Defcon began to repay the affected users by redistributing his commissions, which continued until April (Deepdotweb, 2014). Finally, in November 2014, the market was permanently seized by the FBI (Cox, 2016).

METHODS

Data Collection

Crisis events typically result in a surge of informational activities among the affected members. To identify the period of information surge in the "W" forum, we retrieved posts over the span of two years from January 10, 2014 to March 10, 2016. The data were retrieved from the cyber-intelligence database developed by Cyber-Socio Intelligent Systems Laboratory at Arizona State University. The database system was designed mainly to collect black-hat hacker-related data. For this, the system integrates a data extraction parser and machine learning classifiers to filter out completely non-technical posts such as drug recipes and weapon information. For further information on the designs and development of the system, please see Nunes et al. (2016) and Robertson et al. (2017).

The database is currently operational, actively collecting approximately 305 cyber-threat messages each week from 48 darknet sites (Nunes et al., 2016). The "W" forum data were called from the database by using Application programming interface (API). The data structure of a single hacking post is a JSON-file including the following fields: posting date, sub-board name, topic name and topic ID, post content, user ID. As expected, posting activities abnormally peaked on February 2014, the time of which included the shutdowns of Utopia

and SR2. The rest of our analysis centered on this period, specifically for the one-month period from February 11, 2014 (the day of Utopia Shutdown) to March 12, 2014. This time window covered both Utopia and SR2 crisis, containing 1,693 posts. Fig. 2 shows the three-year longitudinal volume changes of daily posting in the "W" forum.

Analysis Plans

Unitizing. Following Bordia and DiFonzo (2004), we first unitized each post into units of "a complete thought," mostly broken into sentences (p. 37). A "complete thought" unit is defined as "providing enough information that can be interpreted by others and can stimulate a reaction in them" (Wheelan, Verdi, & KcKeage, 1994, p. 44). The 1,693 posts were composed of a total of 7,050 such units. We content analyzed each unit, then aggregated them onto a post level. In this way, we could systematically code the occurrences of multiple types of communication acts in a single post. We then transformed multiple occurrences of the same type within a post into a binary value.

Content Analysis. Communication types were coded based on 10 categories in the CIPHO framework: anxiety, uncertainty, personal narrative, reliance on source credibility/expertise, information providing, deliberation, pro-community, anti-social/disinhibition, procedural directives, and concealment strategies. The intercoder reliability of 10% of thought units were computed, producing a reliable Cohen's Kappa of 0.82. Furthermore, each post was determined whether it was about Utopia crisis, SR2 crisis, or other topics based on the titles and overall themes of discussion threads.

Network Analysis. Based on the content analysis of each post, a multimodal social network analysis – composed of communication types, topical contexts, and users – was used for an overview of the community structure and to identify

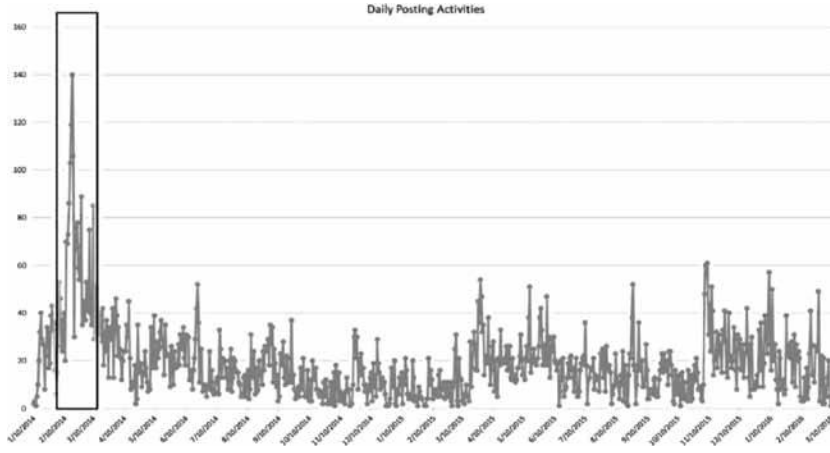

Fig. 2. The Daily Volumes of Posts in "W," Between October 1, 2014 and October 3, 2016. The Period in the Box Was Under Investigation.

key players. A total of 198 users posted at least one message in the "W" forum during the time of investigation.

RESULTS

Overall Posting Activities

Out of 1,693 posts, 143 posts were explicitly about the Utopia crisis, and 449 were about the SR2 crisis. The rest of 1,112 posts were categorized as "non-crisis" topics. Note that we categorized messages as either Utopia- or SR2-related only if the messages were explicitly referring to the SR2 or Utopia crisis context (and related stakeholders). Accordingly, we put any ambiguous messages to the "non-crisis" category. This left a possibility that some messages in this category could be follow-up discussions in response to the shutdowns of Utopia or SR2 even if the messages did not obviously use the words indicative of SR2 or Utopia crisis. For example, the seizure of Utopia could have stirred discussions about overall security; the vulnerability of SR2 could lead users to discuss alternative marketplaces. Specific motivations that drove "non-crisis" messages were unclear, and thus some of non-crisis messages could have resonated with the crisis events as well.

A temporal trend of posting activities showed that most of the Utopia crisis messages occurred in the first four days during the time-period under investigation. The majority of SR2 crisis messages also appeared during early days; however, SR2-related discussions lingered throughout the whole period under investigation. The temporal difference between Utopia- and SR2-related activities could be due to the dissimilar natures of crisis, between the permanent closure of a premature market (Utopia) and the temporary shutdown of an established market (SR2) (Fig. 3).

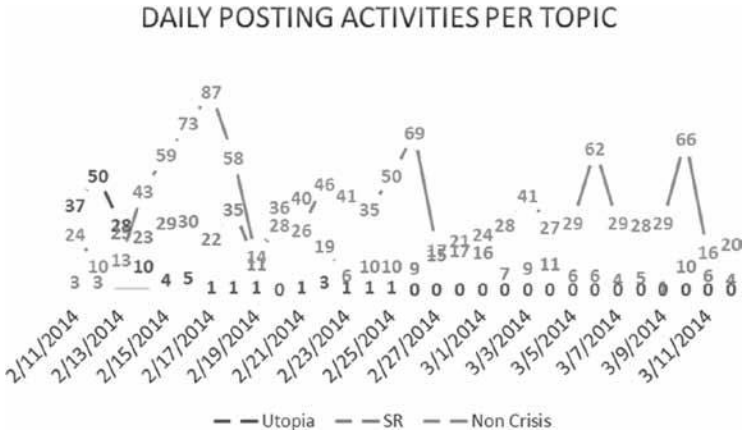

Fig. 3. Daily Posting Activities per Topic in "W," Between February 11, 2014 and March 12, 2014.

RQ1. What communication types were the most salient in the darknet black-hat community under crisis?

In general, rational processing (i.e., information providing and deliberation) were the most prevalent across different topical contexts. That said, the percentage proportions within each communication type showed some differences across three topics. Fig. 4 presents the frequencies as well as the percentage contributions of Utopia, SR2, and non-crisis posts to each type of communication acts.

Kruskal–Wallis *H* tests were used to examine differences in importance of each communication types across the crisis (Utopia and SR2) and non-crisis messages, resulting in significant differences in terms of five types of communication acts: personal narrative, pro-community, anti-social/disinhibition, concealment strategies, and procedural directives (Table 2).

Personal narratives and pro-community were more salient in non-crisis messages than crisis messages. Specifically, personal narratives showed the highest mean rank score of 859.44 for non-crisis messages, followed by 798.12 for SR2, and 775.33 for Utopia, with $\chi^2(2) = 13.71$, $p < 0.01$. Likewise, pro-community showed the highest mean rank score of 857.12 for non-crisis messages, followed by 803.96 for SR2, and 775.69 for Utopia, with $\chi^2(2) = 13.46$, $p < 0.01$. Majority of personal narratives shared users' hands-on experiences with certain vendors, markets, and security technologies. Personal narratives included both positive and negative anecdotes, often encouraging further reviews and feedbacks in non-crisis messages. However, personal narratives concerned with the market shutdowns were mostly negative, which triggered anti-social comments that included blaming, questioning, finger pointing, and name calling. Here, one message exemplifies how a personal narrative accompanies an anti-social comment:

> My wallet was jacked for about $35. I haven't seen one satoshi repaid in my direction. I have ~$60 in pending escrow, haven't seen fuck all from that either. The orders were cancelled, and ta da, you get nothing. SR gets no more of my money until or unless I get mine back. The thing that fucks me off the most is that if I purchase goods from SR, there is the possibility that my money is going to pay off a child molestering, perving scum sucking fuckwit like vIce (another user)[2] I will not.

Whereas pro-community messages were generally common in the "W" forum, the crisis events noticeably increased anti-social interactions. Specifically, anti-social category showed higher mean rank scores for crisis-related messages than non-crisis messages: the highest mean rank score was 903 for Utopia messages, followed by 861 for SR2, and the lowest score of 818.26 for non-crisis messages, with $\chi^2(2) = 41.52$, $p < 0.001$. The anti-social messages expressed distrust, suspicions, and often revengeful messages. For example, one message during the Utopia crisis revealed that the user took advantage of the event to further his self-interest, by violating the darknet community's collective norm (once again):

> I have the codebase and the database for Utopia. In 24 hours I'm going to destroy it, sold or not, because fuck you this isn't a TV show and I don't keep trophies. I'm willing to sell under escrow because I'm not a scammer. 25 btc (bitcoin). You will receive the onion address with a directory that contains a *.tar.gz of both the database I copied when shutting down their

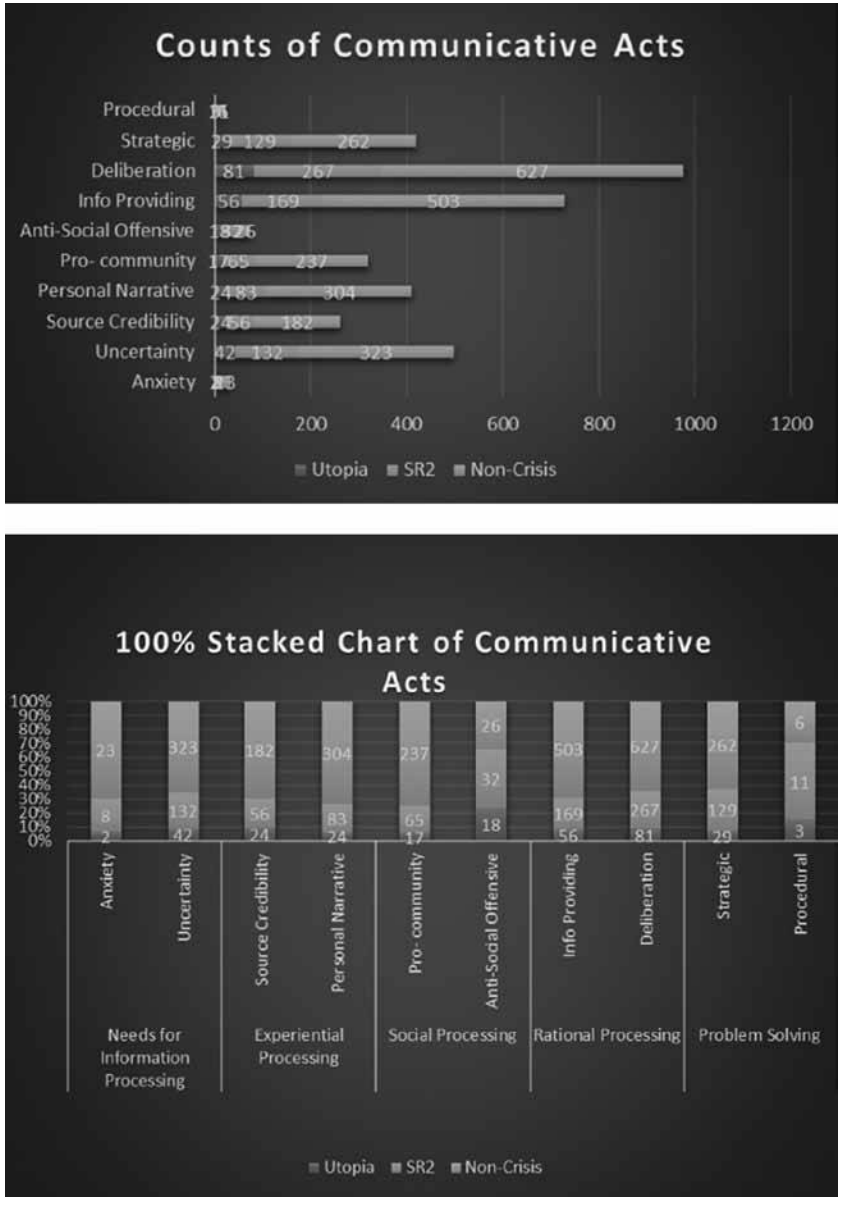

Fig. 4. Frequencies of Communication Types (Top) and Percentage Contributions of Utopia, SR2, and Non-Crisis Topics to Each Type (Bottom).

Table 2. Kruskal–Wallis *H* Test Results.

		Topic	Mean Rank	Chi-Square
Needs for information processing	Anxiety	Utopia	832.11	0.259
		SR2	836.13	
		Non-crisis	837.22	
	Uncertainty	Utopia	832.33	1.301
		SR2	846.33	
		Non-crisis	833.22	
Experiential processing	Source credibility	Utopia	844.25	2.101
		SR2	814.32	
		Non-crisis	843.36	
	Personal narrative	Utopia	775.33	13.711**
		SR2	798.12	
		Non-crisis	859.44	
Anonymous social processing	Pro-community	Utopia	775.69	13.46**
		SR2	803.96	
		Non-crisis	857.12	
	Anti-social/ disinhibition	Utopia	903	41.519***
		SR2	861	
		Non-crisis	818.26	
Rational processing	Info providing	Utopia	799.11	5.749
		SR2	804.1	
		Non-crisis	854	
	Deliberation	Utopia	821.47	4.561
		SR2	872.71	
		Non-crisis	823.61	
Crisis coping	Procedural directive	Utopia	843.92	11.729**
		SR2	847.99	
		Non-crisis	831.06	
	Concealment strategy	Utopia	764.72	13.819**
		SR2	883.11	
		Non-crisis	827.76	

Note: ** $p < .01$, *** $p < .001$

> registration with the passwords already cracked. I will also give you the entire shitty cakephp codebase. Edit: fuck you guys for censoring my sale – isn't that ironic? that you support dark net markets but won't let me sale whatever I want (Apparently, he already violated marketplace rules by posting unwanted content).

Despite aggravated anti-sociality, the community generated significant posts about OpSec, reflective of concealment strategies. The mean rank scores were 883.11 for SR2, 883.11 for non-crisis, and 764.72 for Utopia, with $\chi^2(2) = 13.82$, $p < 0.01$. In contrast to the high occurrences of concealment strategic posts during SR2, the Utopia messages showed the lowest mean rank possibly because the crisis resulted in the permanent shutdown, and thus further actions were pointless for this market. An exemplary message advised other users how to deposit bitcoins securely:

> Services like bitcoinfog mix your coins with other coins. You see btc has a trail so to speak in the blockchain, and you want to fog this trail as much as possible just in case. You don't want to buy btc with your bank account and it ends up linking you to SR. SR used to have a mixing service when your coins were deposited, but it no longer does.

Meanwhile, procedural directives showed higher rank scores for both crisis events (847.99 for SR2 and 843.92 for Utopia) as opposed to non-crisis contexts (831.06), with $\chi^2(2) = 11.73$, $p < 0.01$. Procedural messages occurred more frequently due to the greater need to coordinate discussions under crisis. For example,

> Let's have a discussion here about how to make a secure hidden service, safe from hacks and secure from le. Can it be done, or is the Tor network done for?

Also, procedural directives aimed to reduce anti-social comments against other members:

> There are some honest people on that silk road team. In fact, majority of them are … I respected you until you just blanket-fucked the entire community and staff and I take offense especially after I have just given every coin I had to those who lost out. Go back to writing on that site of yours that nobody reads while the rest of us move on with our lives. If you took that in stride, then pm me, I would like to speak with you one on one.

RQ2. How was communication network in the black-hat community configured based on the CIPHO framework?

A multimodal network was constructed to represent *who* engaged with *which communication types* for *which topic*. Fig. 5 is the social network graph,

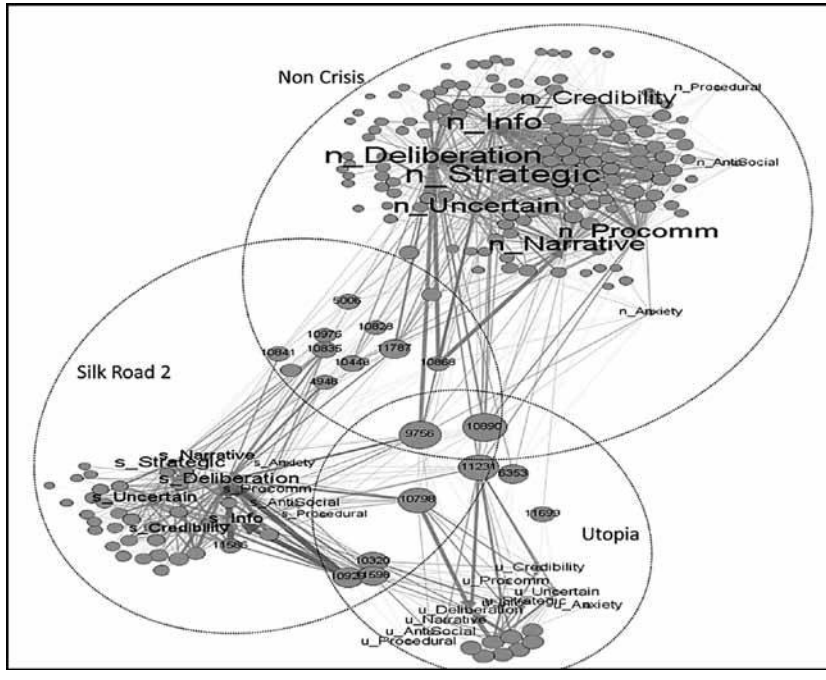

Fig. 5. Communication Network for Silk Road 2 Crisis, Utopia Crisis, and Non-Crisis Topics in the Forum "W" (Visualized with Gephi).

with three clusters of communication types, representative of SR2, Utopia, and non-crisis topics.

Nodes in this graph represented users ($N = 198$) and communication acts for each topic ($N = 30$, 10 per topic). The posts with missing user information were excluded. The labels of communication acts were sized by in-degree centrality, which represented the number of users who posted the given communication type at least once. The node sizes of users were adjusted based on out-degree centrality, which measured the number of different communication types that each user engaged. Note that each user's out-degree centrality reflected the *diversity* of his or her communication activities, not the intensity of each activity type. For example, suppose a user made ten posts of deliberation only during the Utopia crisis while none of any other types. In this case, this user's out-degree centrality should be "1" although the raw count of activities the user made in total was ten. That said, the intensity of activities was represented by the thickness of lines (edges) in the graph.

Several observations are noteworthy. First, the shutdowns of SR2 and Utopia seemed to be in the business interest of only a subset of "W"-members. As the graph showed, many users in the non-crisis cluster did not contribute to SR2 or Utopia crisis topics. These non-crisis posters could be newbies who were not qualified to post in advanced boards. Alternatively, they could be the customers of different marketplaces, given that "W" was a cross-market forum. Half of the users who engaged with the Utopia topic posted messages about the SR2 crisis or other non-crisis topics as well. In contrast, many users in the SR2-cluster were involved in SR2-content, suggesting a possibility that SR2 had established its own loyal customer bases.

Second, several users became prominent by crosscutting topical boundaries. These users could be the key players for disseminating community intelligence for crisis management. For example, the user with ID number 9756 exhibited the highest out-degree centrality in the network, making 26 different types of messages. This user is likely to be a community moderator, inferring from his or her posts that contain procedural messages, for example:

> The W is currently funded only by alvin[3] and the few donations we have received from individual forum members."; "I'm moving this to the silk road subforum – it's more of a concept than breaking news. I think the input of the silk road community would certainly be a useful indicator as to whether your opinion holds weight.

Third, some prominent users engaged with either the same or similar communication activities across different topics. That is, users who showed intensive deliberation activities in one context also exhibited deliberation activities in another context (e.g., user 9756 and 10798). For example, user 10798 contributed prominently both during the SR2 and Utopia crises. Not only did many of his messages include deliberation but also the style of deliberations in both crisis contexts were similar displaying a skeptical tone. In response to SR2 shutdown, for example, this user wrote:

> I feel sorry for you if you actually believe this was anything other than an inside-job. It was most likely defcon who lead the scam but it is possible somebody that worked with him screwed him over but that seems unlikely.

He (she) responded to Utopia crisis in a similar manner, saying:

> I don't believe the part about hiring a hitman. This was said by le and by no one else. Why do you believe everything cops say?

Lastly, among the communication acts, concealment strategy showed the highest in-degree centrality in both non-crisis and SR2 contexts. OpSec messages co-occurred with other message types, implying that they are the outcomes from collective information processing, especially from rational processing of information. Affective aspects such as anxiety and anti-social comments were relatively peripheral.

DISCUSSION AND CONCLUSIONS

Black-hat hackers in darknet are often on the borderline between cyber-libertarians and outlaws. Regardless of different views on their rightfulness, there is a consensus about the importance of understanding organizational workings in their communities. The current study defines black-hat communities in the darknet as one type of hidden collectives, the success of which heavily relies on effective management of organizational visibility and member anonymity. Crisis events like cryptomarket shutdowns can put these communities at risk not only in terms of monetary losses but also failure in managing anonymity. This study examined one of black-hat forums during the two market shutdowns of Utopia and Silk Road 2. Like normal organizations, collective problem solving becomes essential for darknet communities to survive from crisis.

The study analyzed posts in the "W" forum, using the CIPHO framework. The content analysis results suggest a potential for distrust permeating the forum during the marketplace shutdowns. Anti-sociality noticeably increased in crisis-related posts. The increased distrust and offensive comments intensified the tension between high-stakes nature of these crises and limited crisis management resources that solely relies on internal, anonymous sources without access to external help outside the community. Furthermore, members are anonymous to one another, which could have aggravated distrust.

The community's vulnerability seemed to worsen when bitter users violated the rules for anonymity – an essential norm for hidden organizations – for the sake of their own self-interest. As exemplified earlier, one member during Utopia crisis stole the members' identity databases and codebooks, and attempted to sell them, taking the crisis event as an opportunity for revenge. Likewise, although rational processing was prevalent during SR2 crisis (e.g., uncertainty, deliberation, and information providing), such effort often accompanied suspicions and conspiracy theories. SR2-related discussions centered on questioning trustworthiness of the SR2 administrators. The interactions were mostly aggressive, heavily opinionated, and conveyed widespread skepticisms toward SR2 developer teams, even with verbal threats of doxing (e.g., broadcasting personally identifiable information) – a violation of the anonymity rule in the community.

However, such distrust and vulnerability were applicable only to a fraction of the community members. As the communication network showed, not everyone

was a customer of SR2 despite SR2 being one of the major underground markets until 2014. Utopia was too premature to even build its own customer base. Shutdowns of these markets caused high-stake risks for the ones who had been involved in the markets, but not for everyone in "W." Instead, the forum appeared to be fragmented to some degree, offering separate boards for different markets that drew their own customer bases. The fragmentation could be a survival tactic resulting from frequent market-takedowns: as one user pointed out, the darknet has "seen quite number of markets being taken down recently."

Furthermore, black-hat hackers were highly motivated to enhance community security by exchanging concealment strategies. Both in crisis and non-crisis contexts, OpSec messages centrally occurred, intermixed with other communication activities. Users were quick to move on to alternative markets, more secure networks, or different routes to contact vendors. Some users engaged in diverse types of communication activities: they might be key players who bridged fragmented structures.

Our findings conclude that black-hat communities as a hidden organization may be resilient to crisis events thanks to their OpSec strategy-oriented culture and fragmented network structure. That said, anti-sociality was aggravated facing a crisis, leading some users to break the norm of anonymity. Future study may delve further into whether anti-sociality has a causal effect on negating the effectiveness of black-hat hackers' crisis responses. One way to pursue this future direction would be to examine temporal group processes. Our data lacked the temporal information of posts. Missing temporal data prevented us from investigating how communicative activities evolved within each discussion thread. Investigating temporal aspects of CIPHO may offer in-depth insights on how black-hat users collaborate to gain community intelligence for crisis management.

ACKNOWLEDGMENTS

We are thankful to Dr Paulo Shakarian, Soumajyoti Sarkar, and Hunter Priniski for their help. The project was supported by the Office of the Director of National Intelligence (ODNI) and the Intelligence Advanced Research Projects Activity (IARPA) via the Air Force Research Laboratory (AFRL) contract number FA8750-16-C-0112. The US Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright annotation thereon.

DISCLAIMER

The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of ODNI, IARPA, AFRL, or the US Government.

NOTES

1. Per IARPA's recommendation, we do not provide the forum's real name or users' real screennames to avoid any operations security (OPSEC) or future access concerns.
2. See Note 1.
3. See Note 1.

REFERENCES

Abbasi, A., & Chen, H. (2007). Affect intensity analysis of Dark Web forums. In Gheorghe, M., Tayfur, A., Benjamin M., & Daniel, Z. *2007 IEEE Intelligence and Security Informatics* (pp. 282–288). New Brunswick, NJ USA. doi:https://doi.org/10.1109/ISI.2007.379486

Allport, G. W., & Postman, L. (1947). *The Psychology of Rumor*. Oxford, England: Henry Holt.

Barlow, J. P. (1996). *A declaration of the independence of cyberspace*. Retrieved from https://www.eff.org/cyberspace-independence

Benjamin, W. L., Holt, T., & Chen, H.(2015). Exploring threats and vulnerabilities in hacker web: Forums, IRC and carding shops. In *IEEE International Conference on Intelligence and Security Informatics (ISI)* (pp. 85–90), Baltimore, MD, USA.

Bordia, P., & DiFonzo, N. (2004). Problem solving in social interactions on the Internet: Rumor as social cognition. *Social Psychology Quarterly*, *67*(1), 33–49.

Chen, H. (2011). *Dark Web: Exploring and data mining the dark side of the Web* (Vol. 30). New York: Springer Science & Business Media.

Cho, D., & Kwon, K. H. (2015). The impacts of identity verification and disclosure of social cues on flaming in online user comments. *Computers in Human Behavior*, *51*(Part A), 363–372. doi:https://doi.org/10.1016/j.chb.2015.04.046

Coleman, G. (2014). *Hacker, hoaxer, whistleblower, spy: The many faces of anonymous*. Brooklyn, NY: Verso Books.

Cox, J. (2016). The secret life of a silk road 2.0 mastermind. *Motherboard*. Retrieved from https://motherboard.vice.com/en_us/article/3dad83/the-secret-life-of-a-silk-road-20-mastermind

Décary-Hétu, D., & Dupont, B. (2012). The social network of hackers. *Global Crime*, *13*(3), 160–175. Retrieved from https://doi.org/10.1080/17440572.2012.702523

Deepdotweb. (2014). Utopia marketplace seized by Dutch police. Retrieved from https://www.deepdotweb.com/2014/02/11/utopia-marketplace-seized-by-dutch-police/

Epstein, S. (1994). Integration of the cognitive and the psychodynamic unconscious. *American Psychologist*, *49*(8), 709–724.

Fachkha, C., Bou-Harb, E., & Debbabi, M. (2015). Inferring distributed reflection denial of service attacks from darknet. *Computer Communications, 62*, 59–71.

Galbraith, J. R. (1974). Organization design: An information processing view. *Interfaces*, *4*(3), 28–36.

Herring, S., Job-Sluder, K., Scheckler, R., & Barab, S. (2002). Searching for safety online: Managing "trolling" in a feminist forum. *The Information Society*, *18*(5), 371–384. Retrieved from https://doi.org/10.1080/01972240290108186

Holt, T. J. (2007). Subcultural evolution? examining the influence of on-and offline experiences on deviant subcultures. *Deviant Behavior*, *28*(2), 171–198.

Holt, T. J., & Lampke, E. (2010). Exploring stolen data markets online: Products and market forces. *Criminal Justice Studies*, *23*(1), 33–50.

Holt, T. J., Strumsky, D., Smirnova, O., & Kilger, M. (2012). Examining the social networks of malware writers and hackers. *International Journal of Cyber Criminology*, *6*(1), 891–903.

Ionită, M. G., & Patriciu, V. V. (2014). Biologically inspired risk assessment in cyber security using neural networks. *2014 10th international conference on communications* (pp. 1–4). Retrieved from https://doi.org/10.1109/ICComm.2014.6866746

Ionită, M. G., & Patriciu, V. V. (2016). Defending against attacks from the dark web: Using neural networks and automated malware analysis. *International Journal of Computer Science and Information Security*. Retrieved from http://search.proquest.com/openview/937da858408a2897b62c285e6d32d013/1?pq-origsite=gscholar&cbl=616671

Larson, S. (2017). What's next for online black markets? *CNN.com*. Retrieved from http://money.cnn.com/2017/07/21/technology/culture/dark-web-future-alphabay-hansa/index.html. Accessed on November 9, 2017.

Lee, E.-J. (2007). Deindividuation effects on group polarization in computer-mediated communication: The role of group identification, public-self-awareness, and perceived argument quality. *Journal of Communication*, *57*(2), 385–403. Retrieved from https://doi.org/10.1111/j.1460-2466.2007.00348.x

Lee, J. K. (2015). Research framework for AIS grand vision of the bright ICT initiative. *Management Information Systems Quarterly*, *39*(2), iii–xii.

L'Huillier, G., Ríos, S. A., Alvarez, H., & Aguilera, F. (2010). Topic-based social network analysis for virtual communities of interests in the dark web. In *ACM SIGKDD workshop on intelligence and security informatics* (pp. 9:1–9:9). New York, NY: ACM. Retrieved from https://doi.org/10.1145/1938606.1938615

Maddox, A., Barratt, M. J., Allen, M., & Lenton, S. (2016). Constructive activism in the dark web: Cryptomarkets and illicit drugs in the digital 'demimonde.' *Information, Communication & Society*, *19*(1), 111–126.

Mahmood, M. A., Siponen, M., Straub, D., Rao, H. R., & Raghu, T. S. (2010). Moving toward black hat research in information systems security: An editorial introduction to the special issue. *MIS Quarterly*, *34*(3), 431–433. Retrieved from https://doi.org/10.2307/25750685

Marin, E., Diab, A., & Shakarian, P. (2016). Product offerings in malicious hacker markets. *2016 IEEE conference on intelligence and security informatics (ISI)* (pp. 187–189). Retrieved from https://doi.org/10.1109/ISI.2016.7745465

Marin, E., Shakarian, J., & Shakarian, P. (2018). Mining key-hackers on darknet forums. *International conference of data and information sciences* (forthcoming).

Milburn, T. W., Schuler, R. S., & Watman, K. H. 1983. Organizational crisis. Part I: Definition and conceptualization. *Human Relations*, *36*(12), 1141–1160.

Moeller, K., Munksgaard, R., & Demant, J. (2017). Flow my FE the vendor said: Exploring violent and fraudulent resource exchanges on cryptomarkets for illicit drugs. *American Behavioral Scientist*, *61*(11), 1427–1450.

Moor, P. J., Heuvelman, A., & Verleur, R. (2010). Flaming on YouTube. *Computers in Human Behavior*, *26*(6), 1536–1546. Retrieved from https://doi.org/10.1016/j.chb.2010.05.023

Nissenbaum, H. (2004). Hackers and the contested ontology of cyberspace. *New Media & Society*, *6*(2), 195–217. Retrieved from https://doi.org/10.1177/1461444804041445

Nunes, E., Diab, A., Gunn, A., Marin, E., Mishra, V., Paliath, V., …, Shakarian, P. (2016). Darknet and deepnet mining for proactive cybersecurity threat intelligence. *2016 IEEE conference on intelligence and security informatics* (ISI) (pp. 7–12). Retrieved from https://doi.org/10.1109/ISI.2016.7745435

Oh, O., Agrawal, M., & Rao, R. (2013). Community intelligence and social media services: A rumor theoretic analysis of tweets during social crises. *Management Information Systems Quarterly*, *37*(2), 407–426.

Oh, O., Kwon, K., & Rao, H. (2010). An exploration of social media in extreme events: Rumor theory and Twitter during the Haiti earthquake 2010. Proceedings of 31st Int'l Conference of Information System (ICIS) Saint Louis, Missouri, USA, December 12–15, 2010.

Postmes, T., Spears, R., & Lea, M. (1998). Breaching or building social boundaries? SIDE effects of computer-mediated communication. *Communication Research*, *25*(6), 689–715. Retrieved from https://doi.org/10.1177/009365098025006006

Robertson, J., Diab, A., Marin, E., Nunes, E., Paliath, V., Shakarian, J., & Shakarian, P. (2017). *Darkweb cyber threat intelligence mining*. Cambridge: Cambridge University Press.

Runyan, R. (2006). Small business in the face of crisis: Identifying barriers to recovery from a natural disaster. *Journal of Contingencies and Crisis Management*, *14*(1), 12–26.

Scholten, L., van Knippenberg, D., Nijstad, B. A., & De Dreu, C. K. W. (2007). Motivated information processing and group decision-making: Effects of process accountability on information processing and decision quality. *Journal of Experimental Social Psychology*, *43*(4), 539–552. Retrieved from https://doi.org/10.1016/j.jesp.2006.05.010

Scott, C. (2013). *Anonymous agencies, backstreet businesses, and covert collectives: Rethinking organizations in the 21st century.* Stanford, CA: Stanford University Press.

Stark, E., Baldwin, A. S., Hertel, A. W., & Rothman, A. J. (2017). The role of rational and experiential processing in influencing the framing effect. *The Journal of Social Psychology*, *157*(3), 308–321.

Steinmetz, K. F. (2015). Craft(y)ness: An ethnographic study of hacking. *The British Journal of Criminology*, *55*(1), 125–145. Retrieved from https://doi.org/10.1093/bjc/azu061

Suler, J. (2004). The online disinhibition effect. *CyberPsychology & Behavior*, *7*(3), 321–326. Retrieved from https://doi.org/10.1089/1094931041291295

Symantec. (2017). *Internet security threat report 2017* (No. 22). Retrieved from https://www.symantec.com/security-center/threat-report

Wheelan, S. A., Verdi, A. F., & McKeage, R. L. (1994). *The group development observation system: Origins and applications*. Philadelphia: PEP Center Press.

Xu, J., Chen, H., Zhou, Y., & Qin, J. (2006). On the topology of the dark web of terrorist groups. In *Intelligence and security informatics* (pp. 367–376). Berlin, Germany: Springer. Retrieved from https://doi.org/10.1007/11760146_32

Yang, C. C., Tang, X., & Thuraisingham, B. M. (2010). An analysis of user influence ranking algorithms on dark web forums. In *ACM SIGKDD workshop on intelligence and security informatics* (pp. 10:1–10:7). New York, NY: ACM. Retrieved from https://doi.org/10.1145/1938606.1938616

Zhou, Y., Reid, E., Qin, J., Chen, H., & Lai, G. (2005). US domestic extremist groups on the Web: Link and content analysis. *IEEE Intelligent Systems*, *20*(5), 44–51. Retrieved from https://doi.org/10.1109/MIS.2005.96

APPENDIX: DARKNET GLOSSARY

[For more comprehensive darknet dictionary, please find from: https://www.deepdotweb.com/2014/03/02/deepdotwebs-darknet-dictionary]

Blockchain: An ever-growing public ledger operated in digital forms. The ledger publicly stores every page – also known as a block – of transaction records. It is a distributed system managed by a peer-to-peer network, meaning the data in any block cannot be altered without affecting other blocks in the chain. Blockchain is the basis of many cryptocurrencies including bitcoin.

Bitcoin (btc): One of the most popular cryptocurrencies and payment systems.

Bitcoin Fog: One of bitcoin mixing services (or bitcoin laundering services) to cover up bitcoin transaction trails recorded in the blockchain. The service mixes bitcoins of multiple users and pays back to the users through other addresses than the original address. By mixing BTC-transfers of multiple users, the service reduces a chance to prove the connection between the deposit and withdrawal of bitcoins.

CakePHP: An open-source web framework, often used to develop a secure web application.

Exit scam: A fraudulent practice by cryptomarket administrators who steal users' money deposited to the market, by abruptly shutting down the website.

Escrow: A financial transaction procedure that involves a third party to ensure the payment will be transacted once the ordered item is successfully sent to a buyer.

I2P: I2P stands for "Invisible Internet Project," also known as the Garlic Routing. It is one kind of peer-to-peer-network.

LE: LE stands for law enforcement.

OpSec: OpSec stands for "Operations Security," generally defined as a process to protect identifiable information through anonymizing technical means as well as through creation and maintenance of false online personas to prevent identification by the adversary, in this context especially LE.

PGP-Keys: PGP stands for "Pretty Good Privacy," which is an encryption process that allows public transaction of information in a secure manner. The process generates a public–private key pair. A public key is used to encrypt the message to be sent. For example, anyone who has your public key information can send an encrypted email to you. A private key is then used to decrypt the message.

Satoshi: The smallest unit of Bitcoin. Satoshi Nakamoto is also a pseudonym of the inventor(s) of bitcoin.

Tor: TOR stands for "The Onion Router," which is one of the most popular crypto-networks. The network is accessibly only through Tor browser.

Trail: A public record of a digital transfer between sending and receiving addresses, stored in Blockchain.

VPN: VPN stands for "Virtual Private Network." It is a type of network that works as if it were a private network even if the data transaction occurs across a public network. It allows secure and anonymous data transactions.