Crisis and Collective Problem Solving in Dark Web: An Exploration of a Black Hat Forum

K. Hazel Kwon
Arizona State University
Walter Cronkite School of Journalism
Phoenix, AZ
+1 602.496.5268
khkwon@asu.edu

J. Hunter Priniski
Arizona State University
School of Mathematical and Statistical Sciences, Tempe, AZ
+1 602.617.1817
jpriniski@asu.edu

Soumajyoti Sarkar
Arizona State University
CySIS Lab
Tempe, AZ
+1 480.819.7177
Ssarkar18@asu.edu

Jana Shakarian
Arizona State University
CySIS Lab
Tempe, AZ
+1 480.727.6921
jshak@asu.edu

Paulo Shakarian
Arizona State University
CySIS Lab
Tempe, AZ
+1 480.727.5290
pshak@asu.edu

ABSTRACT

This paper explores the process of collective crisis problem-solving in the darkweb. We conducted a preliminary study on one of the Tor-based darkweb forums, during the shutdown of two marketplaces. Content analysis suggests that distrust permeated the forum during the marketplace shutdowns. We analyzed the debates concerned with suspicious claims and conspiracies. The results suggest that a black-market crisis potentially offers an opportunity for cyber-intelligence to disrupt the darkweb by engendering internal conflicts. At the same time, the study also shows that darkweb members were adept at reaching collective solutions by sharing new market information, more secure technologies, and alternative routes for economic activities.

CCS Concepts

• Social and Professional Topics→Computer Crime • Social and Professional Topics→Computing and Business→ Computer supported cooperative work

Keywords

Darkweb; Darknet; Cybercrime; Hidden Organization; Crisis Social Interaction; Collective Problem Solving; Virtual Organization

1. INTRODUCTION

Organizational crisis is defined as a situation that "threatens the high priority goals of [an] organization and restricts the amount of time available for response" [1]. Almost every organization encounters its own moments of crisis that engender uncertainty and anxiety among its members. If organizational members successfully resolve the problem, the organization should survive and even transform the crisis into an opportunity to grow and thrive; if they fail to collaborate and cannot reach collective solutions, however, the organization may incur a significant loss, or worse, cease to exist. Darkweb organizations are no exception.

Activities on darkweb–hacking, data leaks, financial fraud, drug dealing, etc.–are serious causes of crisis to many "normal" organizations, businesses, and communities. Much discussion exists regarding motives of darkweb users (e.g., strategies to enhance cyber-security; socio-cultural dynamics in hacker communities; and tracking criminal networks). However, scholars seem to pay less attention to the premise that the darkweb is in effect a virtual organizing system that has its own moments of instability and crisis.

Understanding the darkweb's crisis problem-solving processes may benefit the cyber-threat intelligence community. The goal of this short paper is to offer preliminary insights on the ways darkweb users collectively interpret crises and reach solutions. We present a case study of one of the forums that gained trust within darkweb society, in the context of the black marketplaces shutdown. A shutdown of a marketplace is one of the most detrimental crises in the darkweb that causes not only significant monetary losses but also physical arrests of organizational members.

As an early stage of the initiative, this study presents content analysis of a small size of discussion posts based on Crisis Information Processing System (CIPS) [2]. Although inspired by previous studies that intended to understand online users' rumour interaction patterns, CIPS includes comprehensive categories of "communicative postures" that may occur in times of crisis, adequately applicable to the current study.

2. BACKGROUND

2.1 Darkweb (Darknet) vs. Clearnet

The terms 'darkweb' and 'darknet' are interchangeably used in this paper. Typically, darknet refers to an earlier and smaller version of crypto-networks accessible only through particular protocols, which are today collectively referred to as the darkweb. Perhaps the most popular crypto-network today is known as Tor (The Onion Router), 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 or "clearnet" hosted sites (if they are not blocking Tor exit nodes), Tor-hosted sites can only be reached with the Tor-browser.

#SMSociety'17, July 28-30, 2017, Toronto, ON, Canada
© 2017 Association for Computing Machinery. ACM ISBN 978-1-4503-4847-8/17/07…$15.00
http://dx.doi.org/10.1145/3097286.3097331

For the past two years, the research team has been identifying and collecting data from websites hosted on several of these networks and network locations that contain information pertaining to malware, data leaks, and financial fraud [3]. The majority of these websites are in English and can be found on Tor as well as on the Surface and Deep Web [4]. The research team has gained valuable insights into behavioural patterns of cyber adversaries [5] and found that many unlawful vendors on the darkweb use identical online handles across multiple disjointed darkweb marketplaces [7].

2.2 Darkweb as a virtual organizing system

One popular misconception about the darkweb is to assume that it is a space predominantly for 'hackers'. This assumption is a categorical fallacy, at least in the context of our study, for two reasons. First, definitions of hackers are multifaceted, ranging from "quirky programmers" [7] to craftsmen [8], to political subversives [9], and to cyber-villains. The social science research community has been interested in a broad spectrum of hackers and their culture, frequently focusing on "white-hat" hackers [10]. To the contrary, this study's interest is centered around the virtual collectives that are organized chiefly for the purpose of illegal activities. Malicious hackers–so called "black-hat" hackers–represent just a small portion of those who claim their identity as a hacker.

Second, the darkweb is *not* a space solely for the purpose of computer hacking. The darkweb is a network of forums (where users collaboratively engage in social interactions, skill development, and problem-solving) and marketplaces (where illegal economic activities occur) [3]. Online forums and marketplaces feed each other, involving not only hackers but also traditional criminals that have connections with street gangs, mafias, and prisoners [11]. Accordingly, often observed in a darkweb forum is the co-presence of various on- and offline malefactors [4, 11].

Therefore, we define the darkweb not as a hacker organization but as a "hidden organization" [12] that interconnects traditional illicit actors and black-hat hackers via a cyberinfrastructure that enables anonymity and security. A hidden organization constantly deals with three organizational issues: organizational visibility, members' identification with the organization, and setting the boundary of relevant audiences [12]. As a hidden organization, the darkweb may well strive to balance these issues between visibility and anonymity, between members' collaboration for collective causes and their pursuits of self-interests, and between broadening their new user-base and prohibiting error-prone newbies.

2.3 Crisis and Problem-Solving Interactions in Darkweb

Considering that the darkweb is built upon anonymous and dispersed cyber-networks, effective computer-supported communication is the key for the darkweb to negotiate these organizational issues. In this sense, the darknet is a "communicatively constituted" [13] organization, whose success relies heavily on message flows and virtual social interaction processes among the members.

Effective message flows and social interactions are especially necessary for the darkweb to survive when facing a crisis. Conversely, from the law enforcement perspective, the deterrence of message flows and social interactions should be an important countermeasure to defeat cyber adversaries. Therefore, understanding social interaction patterns emergent among darkweb users in times of crisis may assist law enforcement to strategize their deterrence endeavors.

To understand patterns of social interactions during darkweb crisis, this study modifies Bordia and DiFonzo's Rumor Interaction Analysis System (RIAS) [2]. RIAS resonates with various communication styles commonly observed under a crisis. RIAS is built upon Krull and Anderson's Explanation theory (1996), a general theory about an individual's cognitive processing when there is a need to make sense of a problematic event [2].

Although Bordia and DiFonzo (2004) focused on rumour communication, the utility and theoretical contributions of their study transcend rumour studies in three aspects. First, RIAS centers on *online* social interactions, offering insights on the development of problem-solving interactions in a cyber or virtual organization such as the darkweb. Second, while Explanation theory centered on an individual's mental processing [2], RIAS applies the tenets of Explanation theory to a *collective* problem-solving situation by addressing ways in which social interactions manifest the collaborative process of sense-making during a crisis. Lastly, as previously mentioned, RIAS includes comprehensive catalogues of "communicative postures" [2] observed in times of crisis, allowing its general applicability to crisis communication contexts beyond rumourmongering per se. Studies have adopted RIAS to explore spontaneous, bottom-up crisis communication in social media context such as Twitter [14, 15].

Therefore, RIAS is adequately applicable to understand collective problem-solving processes emergent within darkweb communities under crisis. We further modified their framework to ensure its universal applicability to online crisis communication, as well as to better serve the purpose of the current study. In doing so, we integrate it with the Heuristic-Systematic Information processing perspective [21]. We refer the modified framework to Crisis Information Processing System (CIPS) hereafter.

3. CASE STUDY: BLACK MARKET CRISES

This study explores black marketplace shutdown as an exemplary case of darkweb crises. A compromise of marketplace's status quo is one of the most damaging crisis events in darkweb society. Marketplaces can be shut down–either permanently or temporarily–due to various reasons such as seizure by authority, technological errors, hacking/theft by other darknet members, or exit-scam. The case we explored traces back to February 2014 when two markets were shut down one after another. These two marketplaces were "Utopia" and "Silk Road 2".

3.1 Market Shutdown 1: Utopia

Utopia was launched on February 3, 2014 (Figure 1) and turned out to be one of the most quickly closed darknet marketplaces. A week after the opening, on February 11, 2014, Dutch Police seized Utopia, along with the bitcoins amounting to $610,900. The Police also arrested five suspects (four Dutch; one German) who allegedly ran the market [16].

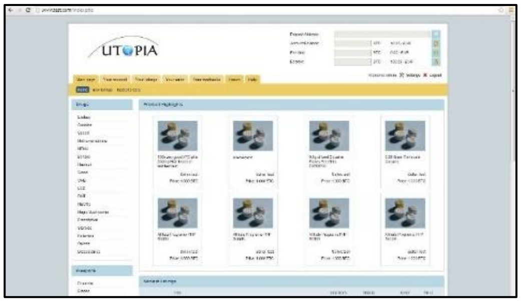
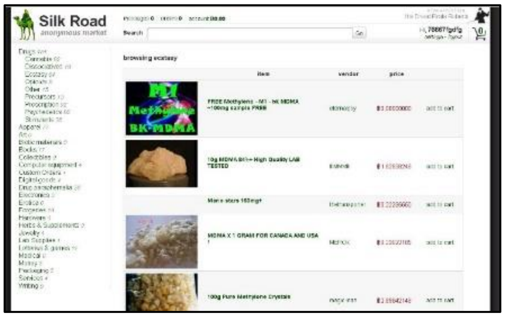


Figure 1. Screenshot of Utopia Marketplace homepage, acquired from deepdotweb.com.

3.2 Market Shutdown 2: Silk Road 2

Silk Road 2 (SR2) was opened on November 3, 2013 (Figure 2). While the original owners of SR2 were arrested in December 2013, the marketplace continued to operate under a temporary administrator with the pseudonym "Defcon". The period this study examined is when 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 [16]. On February 18, 2014, the alleged hackers of SR2 were doxed (i.e., their personal information was leaked, including real names and contact information). Afterwards, the market reopened and Defcon began to repay the affected users by redistributing his commissions, which continued until April 2014 [16]. In November 2014, the market was seized by the FBI [17].



FREE Methylone - M1 - bk MDMA ~100mg sample FREE

10g MDMA 84%+ High Quality LAB TESTED

MDMA X 1 GRAM FOR CANADA AND USA !

100g Pure Methylone Crystals

Figure 2. Screen shot of Silk Road 2 Markeplace homepage, acquired from deepdotweb.com.

4. RESEARCH DESIGN

4.1 Forum "X"

We explored one of the reputed darkweb forums "X"[1] during this period of two market shutdowns. The "X" is a Tor-based forum dedicated to cross-marketplaces affairs and news sharing. It is one of the few communities that allow users to discuss all different marketplaces in one place, without the need to visit a specific market forum separately [18].

4.2 Data Collection

A total of 14,980 posts were retrieved from the forum over the span of three years from January 10, 2014, to March 10, 2016, from the cyber-intelligence system database developed by our research team. We collected the long temporal spectrum of data to see if there is an anomaly in communication volumes, and if such an anomaly coincides with the crisis periods. (Further information on the design and development of the system is available [cf. 3, 19].) This system is "currently fully integrated and actively collecting" the darkweb data on a daily basis [3]. We accessed the system database using an API. The data structure of a single post is a JSON file with variables consisting of: posting time, sub-board name, forum name, post content, and user-name. Due to rate limits with the API, we set up an iterative loop that would repeat the same call continuously until we collected as much data as we needed. The iterative process may result in repetitive data. After deduplication, the dataset included 14,980 posts.

In the "X", posting activities abnormally peaked during the time window from February 11, 2014 (the day of Utopia shutdown) to February 18, 2014 (when SR2 hackers were doxed), which coincided with the period when the shutdown of two markets were serially reported. The simultaneous occurrence of the increase in informational activities and the crisis outbreak is not a surprise: a crisis is a situation where members' interests are put at risk while time and resources needed to resolve the situation are constrained. As a result, a crisis situation is typically characterized by a high level of anxiety and uncertainty–a sufficient condition to generate an irregular surge in information-sharing activities among the affected members. Figure 3 shows the longitudinal volume changes of daily posting in the "X".

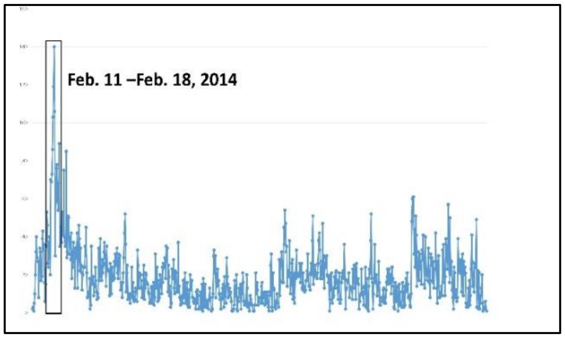


Figure 3. The daily volumes of posts in the "X", between 1/10/2014 and 3/10/2016.

The "X" had 36 sub-discussion boards. Among them, "Flawed Market"[2] was the most populated board during this time window, including a total of 558 posts. This paper focused on social interactions that occurred within this board given its topical relevance and popularity.

4.3 Content Analysis

To understand how problem-solving interactions had been developed in the "X" during the market shutdowns, content analysis was performed using CIPS. The framework includes four dimensions of communication processes that are composed of eight sub-categories of "communicative postures": (i) Need for further interactions (Apprehension and Information needs), (ii) Heuristic processing (Authenticating, Personal narratives), (iii) Social processing (Pro-community sentiment, Trolling/Sarcasm), (iv) Systematic information processing, and (v) Directives.

Following Bordia and DiFonzo's [2] recommendation, we first unitized each post into units of "a complete thought", mostly broken into sentences. A complete thought unit is defined as "providing enough information that can be interpreted by others and can stimulate a reaction in them" [20]. We analyzed each unit-of-thought, then aggregated them onto a post level. In this way, we could systematically code the occurrence of multiple postures in a single post. We recoded multiple occurrences of the same posture within a post into a binary value.

The detailed description of CIAS is presented in Table 1. The intercoder-reliability of 30% unit-of-thoughts was computed based on agreement (89.26%) and Cohen's Kappa (.85).

Table 1. Crisis Information Processing System

Communicative Posture		Definition
Need for interactions	Apprehension	Statements that display fear, anxiety, frustration, etc., caused by the crisis
	Information needs	Seeking information, or a hesitant statement due to the lack of information (e.g., "I'm not sure if it's true", "It may be or may not be true)
Heuristic processing	Authenticating	Adding credibility by referring to external info sources or experts, claiming their own expertise
	Personal narratives	Personal experience or involvement in the context of crisis
Social processing	Pro-community	Community enhancing/supportive statement; an expression of collectivity
	Sarcastic / Trolls	Ridicule someone's belief or statement; Interpersonal attack without reasoning
Systematic Information Processing		Elaborating the information or deliberation by "analyzing, disputing, disagreeing with, and drawing inferences from what someone else had said"; or by justifying one's own views, actions, and beliefs [2, p.42]
Directive		Suggests actionable items, technical solutions, or a course of action

5. RESULTS

Figure 4 shows the frequency of each CIAS category from the analysis of 558 posts in the sub-discussion board, "Flawed Market".

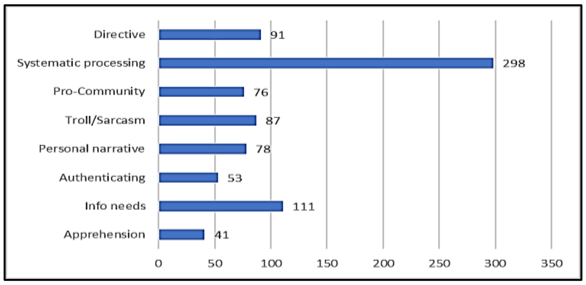


Figure 4. Frequencies of communicative postures

Some noteworthy results are as follows.

1. "Systematic processing" was the most prevalent posture throughout the period. The majority of systematic processing posts displayed members' attempt to interpret causes of the market shutdowns. During the process distrust, suspicion, and conspiracy theories were prevalent. Systematic processing posts were the most cognitively effortful, revealing the seriousness of the events and its potential to cause a deep crack in the community. For example, examining SR2, discussions centered around questioning trustworthiness of the marketplace administrators. Although technical explanations and reasoning were also found in the systematic processing statements (e.g., how the bitcoin protocols had been compromised), interactions were mostly aggressive and heavily opinionated. In general, statements conveyed widespread skepticism toward Defcon and SR2 developer teams. For example, one post stated that *"*[admins] have been spending all of their time telling people to calm down, that their funds would be released… Meanwhile, they constantly reiterated that the developers were focusing on security…Problems were ignored, and the website was chronically understaffed (or so they said)… At best, defcon and the dev team were incompetent…"

2. Members were proactive in suggesting directives. Directive messages were the third most frequently occurring communicative posture. Discussions of technical incompetence led to calls for a rigorous preparation for secure market, for example: "Market owners need to take note! Releasing premature market only damages it in the long run. Stop trying to race it out there."

3. Some communicative postures occurred disproportionately throughout the period, alluding a potent sequential development of collective problem-solving (Figure 5). For example, needs-related statements (apprehension or informational needs) about the event was found most commonly in the early stage of the Utopia crisis, as exemplified by the statement such as: "I'm feeling so useless..."; "very sorry to hear that, man, I know how much time and effort you guys put into it"; "Wat fucking going on with all black markets… maybe can this, the begin of the end?"; Glad I didn't have a chance to place an order yet. Looked promising as a marketplace, unfortunately." On the other hand, this was not the case for SR2, showing the abnormal increase in the emotional and cognitive needs as group interaction progressed.

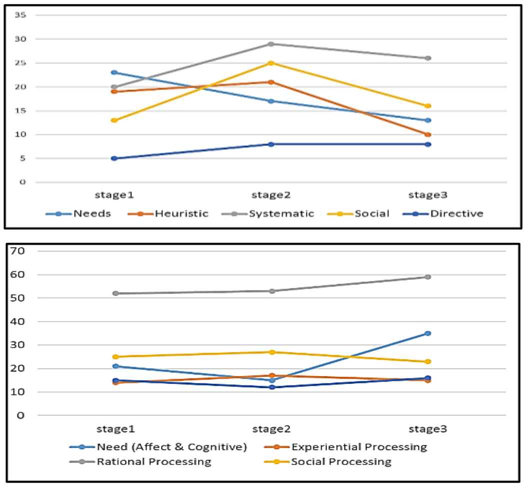


Figure 5. The temporal patterns in "Flawed Market" of Forum "X": Utopia crisis (top) and SR2 crisis (bottom), 2/11 - 2/18/2014

4. One possible reason for this increase at a later stage is because of the increase in informational needs. Unlike previous studies in clearnet contexts, information seeking seems not to be significantly related to authenticating statements. Rather, information-seeking type of statements often came along with systematic processing and directives in our study. This is possibly because the information-seeking postures in Forum "X" mainly sought not factual news updates but internal members' opinions and technological advices. For example, "Can you explain what you mean by vacation mode?"; "been trying to sign up for 3 days but keep getting registration failed??! help?"; "That's all I can think of right now. Please chime in with your suggestion."

6. CONCLUSIONS

This paper presents preliminary findings from content analysis of a darknet forum following the shutdowns of two illegal cyber-market places (Utopia and SR2). Hidden organizations on the darkweb experience their own moments of crises during which collective problem-solving becomes essential for an organization's survival. One notable communicative characteristic this study found is the potential for distrust to permeate the forum during the marketplace shutdown. This may be due in part to their sense-making effort which heavily relies on internal opinions and guesswork rather than verifiable external sources. At the same time, a relatively large volume of directive messages indicates that members were highly motivated to find ways to resolve the issues. Darkweb users seem to move on quickly in search of alternative markets, more secure networks, or different routes to contact vendors. Our findings suggest to the cyber-intelligence community that a darknet marketplace crisis may be an opportunity to win a psychological battle with cyber-criminals by instigating distrust and internal conflicts. Such tactics may be the most effective during the early stages of the crisis, by interrupting darkweb's effort to reach collective understanding of the situation.

7. NOTE

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

2. We also changed the name of the sub-board for the same reason.

8. ACKNOWLEDGMENTS

Some of the authors were supported by AFOSR Young Investigator Program (YIP) grant FA9550-15-1-0159, the Office of Naval Research (ONR) Neptune program and the ASU Global Security Initiative (GSI). Paulo Shakarian and Jana Shakarian are 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 U.S. 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 U.S. Government.

9. REFERENCES

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

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

[3] Nunes, E., Diab, A., Marin, E., Mishra, V., Paliath, V., Robertson, J.J., Shakarian, J., Thart, A., and Shakarian, P. 2016. Darknet and deepnet mining for proactive cybersecurity threat intelligence. *Proceedings of the IEEE Conference on Intelligence and Security Informatics (ISI*) (Tucson, AZ, September 28 – 30, 2016)

[4] Shakarian, J., Gunn, A., and Shakarian, P. 2016. Exploring Malicious Hacker Forums, in Jajodia, S., Subrahmanian, V.S., Swarup, V., and Wang, C. (Eds.). *Cyber Deception: Building the Scientific Foundation*, (p. 259-282), Springer, Switzerland

[5] Robertson, J., Diab, A., Marin, E., Nunes, E., Paliath, V., Shakarian, J., and Shakarian, P. 2017. *Darkweb Cyber Threat Intelligence Mining*. Cambridge University Press

[6] Marin, Ericsson, Diab, A., and Shakarian, P. 2016. Product Offerings in Malicious Hacker Markets. In *Proceedings of the IEEE Conference on Intelligence and Security Informatics (ISI)* (Tucson, AZ, September 28 – 30, 2016)

[7] Nissenbaum, H. 2004. Hackers and the contested ontology of cyberspace. *New Media & Society*, 6(2), 195-217.

[8] Steinmetz, K. F. 2014. Craft (y) ness: An ethnographic study of hacking. *British Journal of Criminology, 55* (1), 125-145.

[9] Coleman, G. 2014. *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous*. Verso Books.

[10] 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.

[11] Goodman, M. 2015. *Future Crimes: Everything is Connected, Everyone is Vulnerable and What We Can Do about It*. Random House.

[12] Scott, C. 2013. *Anonymous Agencies, Backstreet Businesses, and Covert Collectives: Rethinking Organizations in the 21st Century.* Stanford University Press.

[13] Stohl, C., & Stohl, M. 2011. Secret agencies: The communicative constitution of a clandestine organization. *Organization Studies,* 32(9), 1197-1215.

[14] Oh, O., Agrawal, M., & Rao, H. R. 2013. Community intelligence and social media services: A rumor theoretic analysis of tweets during social crises. *MIS Quarterly*, 37(2), 407-426.

[15] Oh, O., Kwon, K. H., & Rao, H. R. 2010.An Exploration of Social Media in Extreme Events: Rumor Theory and Twitter during the Haiti Earthquake 2010. *Proceedings of ICIS* (Aug. 2010), 231-240.

[16] Deepdotweb (2014). Utopia marketplace seized by Dutch police: 5 arrested. *DeepDotWeb*. Retrieved from https://www.deepdotweb.com/2014/02/11/utopia-marketplace-seized-by-dutch-police/

[17] Cox, J. (2014). How Silk Road bounced back from its multimillion-dollar hack. *Motherboard*. Retrieved from http://motherboard.vice.com/read/how-silk-road-bounced-back-from-its-multimillion-dollar-hack

[18] Cook, J. 2014. FBI arrests former space X employee, alleging he ran the 'deep web' drug marketplace Silk Road 2.0. *Business Insider*. Retrieved from http://www.businessinsider.com/fbi-silk-road-seized-arrests-2014-11

[19] J. Robertson, A. Diab, E. Marin, E. Nunes, V. Paliath, J. Shakarian, P. Shakarian. 2016. Darkweb mining and game theory for enhanced cyber threat intelligence. *Cyber Defense Review 1*(2), 95-121.

[20] Wheelan, S. A., Verdi, A. F., & McKeage, R. L. 1994. *The Group Development Observation System: Origins and Applications*. PEP Center Press.

[21] Chaiken, S., & Maheswaran, D. 1994. Heuristic processing can bias systematic processing: Effects of source credibility, argument ambiguity, and task importance on attitude judgment. *Journal of Personality and Social Psychology*, *66*, 460-46.