Proceedings of the 53rd Hawaii International Conference on System Sciences | 2020

Knowledge Sharing Network in a Community of Illicit Practice: A Cybermarket Subreddit Case

K. Hazel Kwon
Arizona State University
khkwon@asu.edu

Weiwen Yu
Arizona State University
weiwenyu@asu.edu

Steve Kilar
Arizona State University
skilar@asu.edu

Chun Shao
Arizona State University
cshao9@asu.edu

Kailey Broussard
Arizona State University
kcbrouss@asu.edu

Thomas Lutes
Arizona State University
tnlutes@asu.edu

Abstract

Often neglected in the literature about communities of practice is the fact that online knowledge-sharing communities thrive among illicit collectives whose activities are stigmatized or outlawed. This paper focuses on a knowledge-sharing community of users who engage in illegal practices by examining the ways in which the community's network structure changes when a high-stakes, uncertain event—the July 2017 shutdown of the dark web market Alphabay—occurs. This study compares the discussion network structures in the subreddit r/AlphaBay *during pre-shutdown days (the "routine" period) and shutdown days (the "market defect" period) and offers a content analysis of the knowledge and resources shared by users during these periods. Several differences were observed: (a) the network structure changed such that the network size grew while becoming more centralized; (b) new crisis-specific players emerged; (c) types of knowledge shared during the market defect period was qualitatively different from the routine period.*

1. Introduction

Knowledge sharing communities are commonplace in digital spaces. Decades of literature has explored motivations for and effectiveness of knowledge collaboration online in various contexts such as business [1, 2], distributed software development [3—5] and e-learning [6—8].

Studies on virtual knowledge sharing have largely centered around the notion of "communities of practice," an informal group of people who share knowledge, resources, and meaning, and collectively learn how to solve problems or do the work better [9]. Most studies of knowledge collaboration examine online communities of lawful practices. Often neglected is the fact that online knowledge sharing communities exist, and thrive, for illicit collectives whose activities are stigmatized or outlawed [10].

Illicit knowledge sharing communities are mostly hosted in a hidden side of the digital world: the dark web, a collection of websites and web services that are accessible only through an anonymizing browser (e.g., Tor) or special routing software (e.g., I2P). Not all activities in the dark web are harmful. In fact, some dark web activity helps expand civil liberties, challenging an institutionalized, governmental, or otherwise rigid notion of "legitimacy" [11]. The dark web often serves as the most secure channel for free speech, offering space for journalists, whistleblowers, and political dissidents who challenge repressive regimes [12, 13].

Nonetheless, much dark web activity is dedicated to transactions involving illegal products (e.g., drugs and weapons), cybercrimes (e.g., malware and cyber-frauds), and the circulation of harmful content (e.g., child pornography). The ecology of communities of illicit practices is complicated by the fact that some dark web-related content is visible in the surface web (e.g., subreddits, news aggregator sites). However, information exchanges that occur within communities of illicit practices almost always use anonymization technologies to conceal identities, regardless of whether the community operates only in the darknet or is visible in both the dark and surface web.

This paper focuses on knowledge sharing communities of dark web users who engage in illegal economic practices. Specifically, we define a cyber-underground market community as a self-organized community of practice and examine the ways in which the community's knowledge sharing network structure changes when a high-stakes, uncertain event occurs. Illegal markets have been one of the most troubling cybersecurity issues concerned with dark web

URI: https://hdl.handle.net/10125/64076
978-0-9981331-3-3

activities, and thus worth the empirical attention. The empirical case of interest is the subreddit community *r/AlphaBay*, which was dedicated to discussing a cryptomarket called AlphaBay. AlphaBay, which became the biggest cyber-underground market, operated from December 2014 until July 2017, when it was compromised and permanently shut down by law enforcement [14]. This study compares the discussion network structures in *r/AlphaBay* during pre-shutdown days (the "routine" period) and shutdown days (the "market defect" period). This study also offers a content analysis of the types of knowledge and resources that were shared by users during these periods and how members' communicative activities differed during the two periods.

2. Illicit Cybermarket Communities in the Dark Web

The existence of cryptomarkets in hidden parts of the web has become widely known to the public since the seizure of the infamous cyber-underground marketplace SilkRoad by the Federal Bureau of Investigation in October 2013. Research has found that illicit drugs comprise the most common products exchanged in cryptomarkets, followed by stolen data [15, 16]. AlphaBay was no exception: A vast portion of online discussions about the AlphaBay market alluded to illegal drugs.

Virtual information sharing to assist drug transactions is arguably older than the Internet. Stanford University and MIT students struck a deal regarding a marijuana sale in the early 1970s through the ARPANET, the Internet's predecessor [17]. In the 1980s and 1990s, a forum known as *alt.drugs* existed in Usenet for drug-related discussions [17]. Early cyber drug markets such as AdamFlowers were based on encrypted email accounts and relied on monetary transactions via Western Union, Paypal, Pecunix, I-Golder and cash [18].

Illicit market transactions in the early days were sometimes traceable, making it was easier for law enforcement to detect the involved actors [18]. The rise of anonymizing technologies such as Tor, Virtual Private Network (VPN), and cryptocurrency enhanced the security of transactions, contributing to the expansion of the illicit digital economy. As of April 2019, 11 retail markets and seven vendor shops were listed as English-based marketplaces on deepdotweb.com, one of the main news sites for dark web market users. Although the status of those marketplaces may fluctuate (e.g., being offline, online, or temporarily unavailable), they are active markets. While drugs are the most common products in these markets, other commodities such as weapons, illegal services, hacked data, and malware are also sold.

If marketplaces are one pillar of the cyber-underground economy, the other pillar is discussion forums [19]. Given the instability of market platforms, the sustainability of the cyber-underground economy depends on timely information sharing among market members to help assess vendor and platform credibility and security updates. Beyond the whole market being compromised, even a single individual's identity breach can increase the collective risk. Therefore, community members tend to be proactive with respect to sharing knowledge about identity concealment strategies, called OPSEC [20—22]. Vendors and users often maintain the same screen name across different marketplaces and forums as a trust-building mechanism [19]. Participation in discussion forums helps contributors advertise products, demonstrate expertise, and gain visibility as reliable informants. A positive reputation established in discussion forums can function as social capital [23] that may translate into higher economic returns.

3. Illicit Cybermarket Communities as Self-Organized Communities of Practice

Considering the role online forums play in the illicit cybermarket ecology, an examination of the network structures in these forums may help explain how cybermarket users engage in knowledge sharing to pursue their collective interests. Accordingly, we propose to conceptualize illicit cybermarket forums as self-organized communities of practice.

The characteristics of illicit market forums fit incredibly well the definition of communities of practice. Communities of practice are defined as "groups of people informally bound together by shared expertise and passion for a joint enterprise" [24, p. 139]. Communities of practice have become an integral part of organizational systems that require some level of collective knowledge management, including business, government, education, and social sectors [25]. Online networks help create decentralized communities of practice that are larger scope and size. The ways in which hidden cyber-collectives exploit digital platforms are commensurate with essential features of communities of practices [24, 25].

3.1. Purposiveness

A community of practice "is defined by a shared domain of interest" [25, p.1]. The illicit market actors share a clearly defined agenda: to engage in economic activities that are stigmatized or outlawed by legitimate

institutions. Due to the nature of illegitimacy, members also share another problem: OPSEC. Specifically, the interests in OPSEC have evolved at two levels. At the "system level," market platforms are vulnerable to the risks of hacking, theft, and infiltration by law enforcement; at the "process level," vendors can deceive buyers (e.g., not shipping a promised product) [15].

3.2. Practice

A community of practice is where members learn about "*becoming* a practitioner, not learning *about* practice" [26, p.48, *italics* original]. Therefore, the process of knowledge sharing in communities of practice is oriented toward pragmatic, experiential learning. The illicit market forum members have a shared goal of becoming a "successful" practitioner: buying or selling drugs without being busted. The primary aim of the forums, therefore, is to document and exchange technical and practical knowledge needed to securely participate in high-stakes activities. Other motives such as punditry, leisure, or socialization may be observed but they are auxiliary drivers of social interactions in these forums.

3.3. Knowledge Embedded in Social Interactions

Learning is the main function of communities of practices [9]. Unlike formal training or structured teaching, knowledge is gained through informal social interactions in which not only "objective" knowledge but also, and more importantly, "insider" know-how is embedded [26, p.48]. Learning in communities of practice thus translates to internalizing the culture of collectives such as viewpoints, vernaculars, and behavioral rules [26].

The dark web market forums are where market users with different levels of experience get together to share with and learn from peers' knowledge and experiences. While some forums include well-formatted technical tutorials on how to use markets, the largest portion of communicative activities observed in these forums is in the form of real-time questions and answers [20]. Novices seek tips and advice; experienced users share previous experiences, which in turn constitute a collective narrative of the dark web market history; the involved members share up-to-date information about markets' status and share vendor reviews. Such learning occurs in the midst of informal discursive interactions.

3.4. Self-selection

A community of practice is not a formal organization. Unlike project group assignments or organizational divisions, members voluntarily choose to be a part of the community [24]. Individual members' positions in the community are thus determined not hierarchically but based on the level of time and effort they spend in the community at their own will.

Such informality and meritocracy are defining characteristics of dark web market forums [20]. Whereas actual marketplaces are run by more or less canonical rules (e.g., imposing mechanisms of social control and administrative authority to ban certain vendors and buyers), most discussion forums are run as an open, self-regulated network of voluntary members. The level of expertise, experience, or technical sophistication are not criteria for membership, although there is an implicit expectation that a user should achieve some level of expertise through both informal learning in forums as well as actual engagement in market activities to become a true member of the community.

3.5. Self-organized Knowledge Collaboration

Based on informal social interactions and self-selective membership, communities of practice can be understood as a *self-organized* knowledge sharing system. An essential characteristic of a virtual self-organizing system is its fluidity [27]. A fluid organizing system lacks traditional structural mechanisms such that organizational positions, roles, and boundaries are loosely defined [27]. Instead, fluidity allows "highly flexible and permeable boundaries" of communities, making it difficult "to figure out who is in the community and who is outside at any point in time, let alone over time" [p.1226]. Furthermore, the dynamics of knowledge collaboration do not rely on predefined role structures or adhesive "people-to-people relations" [p.1235]. Rather, the collaborative network changes its configuration constantly based on the flow of ideas, external conditions, and the nature of problems that the community collectively encounters. Scholarship has referred to such organizational flexibility for knowledge collaboration as "emergent network" [28—30] or "generative response" [27].

The dark web market forms are a space for fluid collectives in that there is no strict protocol to enter and exit, insofar as a user has a basic ability to get access to it anonymously. Although administrators may moderate community interactions to some extent, the community does not impose a formal hierarchy. Anonymous social interactions make the community even more permeable because members' real identities

are concealed from one another and thus social interactions are assumed to be inherently temporary and transitory [31].

In sum, as a self-organized system, knowledge sharing dynamics in illicit market forums can be highly adaptive to the nature of problems, level of uncertainty, and who has what types of knowledge at a given moment. Given that few studies have examined the emergence of knowledge sharing networks in the dark web market forums, the current study attempts to contribute to understanding the self-organizing aspect of these communities.

4. Empirical Context and Research Questions

This study presents a case of the cryptomarket called AlphaBay. AlphaBay was shut down in July 2017. Initially suspected as an exit scam (i.e., a fraud by the market administrators), it later turned out that the shutdown was caused by an international law enforcement team comprised of the U.S., Canada, and Thailand. On July 15, 2015, Alexandre Cazes, a co-founder of the market who was arrested on the same day as the shutdown, was found dead in jail in Thailand. AlphaBay was the largest cyber-underground market to emerge since the shutdown of the legendary market SilkRoad, with $600,000 to $800,000 in daily revenue.

Several major forums served as communities of practices for AlphaBay users, including *AlphaBayfrm* (an AlphaBay market-specific forum hosted in Tor), *The Hub* (a multi-market forum hosted in Tor), and several subreddits on Reddit.com. This paper focuses on one of the subreddit communities, *r/AlphaBay*.

This paper is particularly interested in the emergent network structure of the illicit market forum. As a self-organized knowledge sharing collective, the community dynamics may reveal fluid knowledge flows depending on the types of problems that users collectively face. Specifically, in ordinary times, the problems users encounter may be more routinized, centered around vendor credibility and procedural issues related to access, transactions, and shipping. However, when a system-level defect in the market platform is abruptly experienced, the non-routine situation may pose more severe collective risks with a higher level of uncertainty. Facing a non-routine, highly uncertain event could change the interaction dynamics.

We contend that such change should be manifest in two forms: (a) We anticipate changes in communication network structures. According to communication network evolution perspective, a crisis event plays a role in changing the structure of computer-mediated communication networks. For example, a study of an inter-organizational email network showed that both communication volumes and number of communicators have increased when members faced an organizational uncertainty. Also, the network tends to form a giant component rather than being fragmented into subgroups [32]. More recently, Twitter research in the context of natural disaster (Japanese earthquake and Tsunami) found that affected users (i.e., Japanese users) intensified their degree of interactions than non-affected users (i.e., non-Japanese). Such interactions, however, have increased among the existing users, with less activity of newly joining or quitting a community [33]. (b) Along with network change, the nature of communicative content shared among members may also change. For example, prior research has shown that, along with the average length of individual messages being shortened, conversations became less diverse and more concentrated toward problem-solving [32, 33]. Also, decentralized problem-solving efforts and concerns about safety and wellness of community members became prominent in the electronic messages exchanged during the crisis period [34]. While existing studies were based on legitimate communities or organizational networks, little is known whether illicit, hidden cyber communities will exhibit similar patterns in network changes and communication contents when they face a highly uncertain situation. As a preliminary study, this paper posits two research questions.

RQ1: How does the structure of the knowledge sharing network change in an illicit market forum when the community collectively experiences a critical market defect?

RQ2: How do communicative activities change in an illicit market forum when the community collectively experiences a critical market defect?

5. Methods

5.1. Data Collection

The subreddit data (*r/AlphaBay*) was provided by a cybersecurity firm that has partnered with the university where the authors are affiliated (Company name will be identified upon the paper acceptance). Whereas mainstream media reported that AlphaBay was seized on a specific day (July 4, 2017), the market users' experience was not a one-day event. Instead, users experienced errors and irregularities for multiple days around the time of the seizure. To identify the timespan of the market defect more precisely, we

adopted a previous study's method that was used to detect the anomaly period in social media activities [35].

Specifically, we first examined the longitudinal pattern of daily posting volumes over a year, from June 2016 to July 2017. The daily average of total posting was 48.48 posts a day (SD=62.34) and the daily average number of newly created topic threads was 6.03 (SD=5.73). Second, we used the number of newly created topic threads as a criterion to identify the anomaly in activity volumes. We used the topic threads instead of total post activities because it is possible that a certain old topic could continue to draw conversations over time regardless of the shutdown event. Beginning a new discussion thread, however, may be more reflective of what is happening at a given moment. Next, we defined days were considered part of the anomaly period if a daily number of newly created topic threads exceeded two standard deviations from the mean (=17.50). Lastly, we reviewed the actual posts made during the identified anomaly days to understand what had happened and whether the happening was indeed related to a non-routine problem with a high level of uncertainty.

From the procedure above, we identified two abnormal periods, one in December 2016 and another in July 2017. The review of the posts suggested that the market was offline temporarily on December 13 and 14, 2016; and the market defect, which eventually was linked to the permanent shutdown, was experienced for about 10 days from July 5 to July 14, 2017 (Figure 1).

This study focuses on the identified ten days of the market defect in July 2017. The total number of topic threads that were created during the market defect period was 346, and the total number of posts was 1,587. For comparison, we also examined a similar number of topic threads and posts made prior to the beginning of the market defect period, which spanned from May 19, 2017, to July 4, 2017. We defined this time window as a "routine period," which included the creation of 383 topic threads and 1,663 posts. As a result, a total of 3,250 posts were analyzed.

5.2. Network Analysis

Network analysis requires two sets of variables: nodes and edges. In this study, nodes are anonymous users involved in discursive activities in the examined subreddit forum. Edges are defined as non-directional ties that represent co-posting behaviors. The default format of the network data was a two-mode (user-by-thread) matrix that informs which users contributed to which topic threads. The default format was transformed into a one-mode (user-by-user) sociometric matrix based on co-postings in the same topic threads (Figure 2a and 2b).

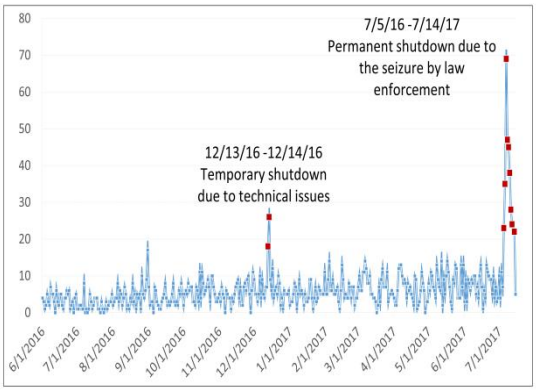

Figure 1. Daily creation of topic threads between June 2016 and July 2017. Red markers are the days with a sudden increase in volume (> 17.5).

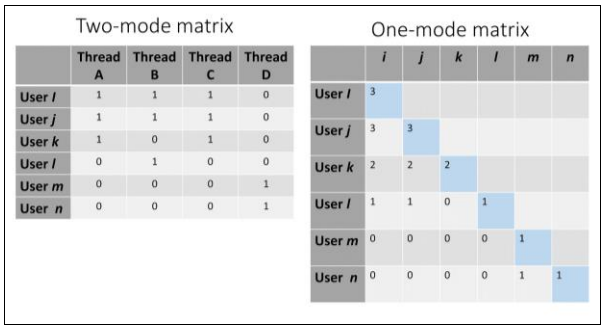

Figure 2a. An example of transforming a two-mode (user-by-thread, directional) matrix to the corresponding one-mode (user-by-user, nondirectional) network. Diagonal values (blue cells) in the one-mode matrix indicate each user's total posting frequency.

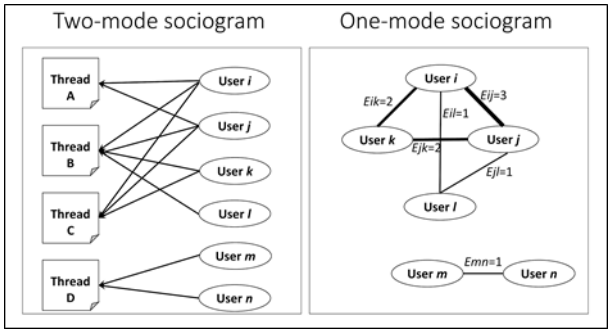

Figure 2b. Sociograms of two-mode network vs. one-mode network based on the sociometric data exemplified in Figure 2a.

The co-posting matrix is more useful in this study than the original user-by-thread matrix because it allows for examining who were exposed to whose ideas/knowledge as well as who were the most active contributors *across* different topics.

That said, the transformation of a two-mode network into a one-mode network loses one important property of the data: the absolute total number of posts that a user contributed. For example, suppose users *i* and *j* contributed one post to the same thread A. The co-posting-based edge weight between user *i* and *j* would be 1 (*Eij*=1). If user *i* made three posts across three different topic threads A, B, and C, and user *j* also made three posts across the three same threads A, B, and C, the edge weight between *i* and *j* would be 3 (*Eij*=3). However, if user *i* made three posts across threads A, B, and C, while user *j* also made three posts yet only in thread A, the co-posting-based edge weight between *i* and *j* will be just 1 (*Eij*=1) even if user *j*'s total number of posts was 3. Furthermore, suppose user *i* made three posts across threads A, B, and C, whereas user *j* made three posts across D, E, and F. In this case, their co-posting-based edge weight will score zero (*Eij*=0) irrespective of how many contributions each user has made.

Considering that the one-mode transformation engendered the loss of the total posting information, we created a node attribute that indicates the total number of posts a user contributed across all topic threads during each period (i.e., routine and market defect period). As presented in a later section, we used both co-posting-based degree centrality and the total post frequency as key performance indicators (KPI).

5.3. Content Analysis

Considering that an essential goal of communities of practice is knowledge sharing for problem-solving, we analyzed whether a post contains *strategic assessment* that helps improve the situation or solve problems. Organizational uncertainty management literature suggests that group members reduce uncertainty in two ways. First, they collectively make sense of the status of the situation (e.g., how likely the concerned outcome is to occur or how severe the outcome would be) [33]. The group information processing perspective [34] defines such type of uncertainty management as "closure," which refers to reaching a conclusion of how to define the state of the situation. Second, community members manage the uncertainty by sharing specific resources and knowledge that help identify what actions should be taken to appropriately respond to the situation or problems [33].

Based on the literature, a post was defined as containing a strategic assessment if the message had a conclusive statement that definitively diagnosed the situation or if the user suggested actionable item(s) to resolve or improve the situation or problems. About 10% of the posts were analyzed for intercoder reliability, reaching 90.23% agreement and a Cohen's Kappa coefficient of .685, suggesting substantial agreement.

6. Results

6.1. Network Structure Overview

The number of posts included for the market defect period (=1,587) was less than the routine period (=1,663). Nonetheless, the co-posting network analysis revealed that *more* users and *more* co-posting edges were included in the market defect period than the routine period. Specifically, 709 users created 24,320 co-posting ties during the market defect period, whereas 592 users created 6,296 ties during the routine period. The large number of co-posting ties also resulted in higher average degree centrality (weighted) during the market defect period (=36.181) than the routine period (=11.196)

Conventionally, a network tends to have a lower density as its size grows because density is computed against the total number of all possible edges. This was not the case in this study, however. Even if there were more users involved in discussions during the market defect period, the co-posting activities were so extensive that the network density (=.048) was also noticeably higher than the routine period (=.018).

Along with density, other structural characteristics similarly suggested that the market defect period showed more *concentrated and centralized* knowledge sharing patterns than the routine period, including a shorter network diameter and shorter average path length, and a larger clustering coefficient and larger centralization coefficient. Table 1 compares the network structural characteristics between the routine and market defect period. Also, Figure 3a and 3b visualize the co-posting network structure configured in each period.

Table 1. Co-posting network analysis results.

Network properties	Routine	Market Defect
# of posts included	1663	1587
# of nodes	592	709

# of edges	6296	24320
Avg. degree (weighted)	11.196	36.181
Network diameter	9	7
Graph density	.018	.048
Avg. clustering coefficient	.797	.826
Avg. path length	3.492	2.771
Centralization (degree)	.236	.474

6.1. Key Players Identification

Degree centrality and total posting frequency were used as KPIs to identify "key players" in each time period. Specifically, we first selected the top 10% of users based on the degree centrality during the routine and market defect period, respectively. Then we selected another top 10% of users based on the posting frequency during each time period. Some users had both high degree centrality and posting frequency and thus were selected repeatedly. As a result of using both KPIs, we identified a total of 174 key players. Eighteen (10%) of these key players appeared in both routine and market defect periods, 64 (37%) were associated only with the routine period, and 92 (53%) uniquely emerged during the market defect period. In other words, those who emerged as active participants during the market defect period were *different* users from those active during the routine period.

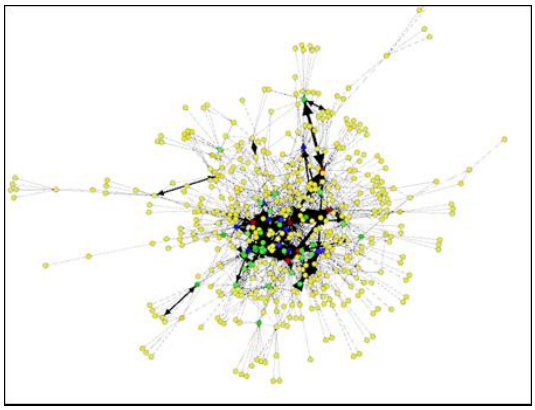

Figure 3a. Co-posting network during the routine period. Nodes are colored based on degree centrality, with red (>= 150), blue (100-149), green (50-99), and yellow (< 50).

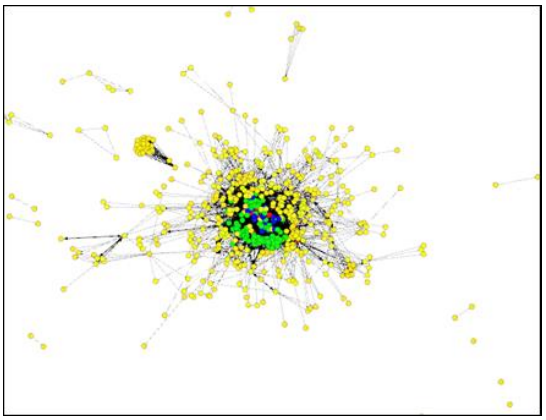

Figure 3a. Co-posting network during the market defect period. Some peripheral nodes were removed from the visualization. Nodes are colored based on degree centrality, with red (>=150), blue (100-149), green (50-99), and yellow (< 50).

6.2. Knowledge Sharing for Strategic Assessment

The content analysis resulted in 356 posts that contained strategic assessment during the routine period (21.4% out of 1663 posts) and 369 posts during the market defect period (23.25% out of 1587 posts). Although key players constituted only a small fraction of users engaged in each period, they were incredibly active in sharing strategic knowledge in both periods, accounting for 55% (post *N*=198) of the total strategic knowledge sharing during the routine period and 57% (post *N*=210) during the market defect. The rest of strategic knowledge sharing was contributed by non-key players (Table 2 and Figure 4).

Table 2. Strategic assessment posts made by key players (KP) and non-key players.

	Routine		Market Defect	
	User *N*	Post *N*	User *N*	Post *N*
All-time KP	18	44 (12%)	18	49 (13%)
Period-specific KP	64	154 (43%)	92	161 (44%)
Non KP	510	158 (45%)	599	159 (43%)
Total	592	346 (100%)	709	369 (100%)

The distribution of strategic knowledge sharing across the three user types—all-time key players, period-specific key players, and non-key players — were similar between the two time periods. In other words, the proportion of contributions from each group was consistent between the routine and market defect period.

However, when the actual messages were reviewed, the nature of shared knowledge was distinctive between the two time periods. Specifically, during the routine period, the strategic knowledge sharing was centered around (a) how to use AlphaBay securely, e.g., *"if you are using ab without a vpn then your isp already knows what you're doing. If you have a vpn then net neutrality elimination shouldn't be a significant problem"*[1]; (b) information related to shipping and transactions, e.g., *"paper is a hard thing to find among thousands of other packs of paper."* [2]; and (c) vendor information, e.g., *"if you don't mind international then gammagoblin with over 250$ spent gets tracked so you have that safety."*

Meanwhile, during the market defect period, the attempt for closure was made by concluding Alphabay's shutdown was an exit scam, e.g., *"... it's looking more and more like they've fucked us. for me i lost quite a bit mid purchase. but nowhere near as much as some people.. if they stay down it'll ruin lives. be nice. help find vendors. do what you can because some people might have really fucked up."* It was only after July 12 when the correct conclusion was reached that the shutdown was caused by law enforcement, e.g., *"Alphabay taken down by law enforcement across 3 countries...lol...yes. It was official yesterday really. There is no hope for alpha whatsoever."* Another chunk of strategic assessment in this period related to alternative markets or routes for transactions, e.g., *"Hansa [market] is so much safer. You are probably a vendor which is why you are supporting Dream market."*

In both routine and market defect periods, security-related discussions such as the importance of VPN, encryption, and running the privacy program Tails with a virtual machine, recurred consistently, e.g. *"the biggest silver lining with alphabay going away is now you get a nice reset on your opsec…i'll send it unencrypted and just trust this handy little checkbox to do the hard work for me? at least those unencrypted messages are likely no longer a risk as le will probably...move on as well like us to the next active market."*[3]

[1] ab = AlphaBay; isp = Internet Service Provider.

[2] paper = an ingestible form of drug tablet

[3] le = law enforcement

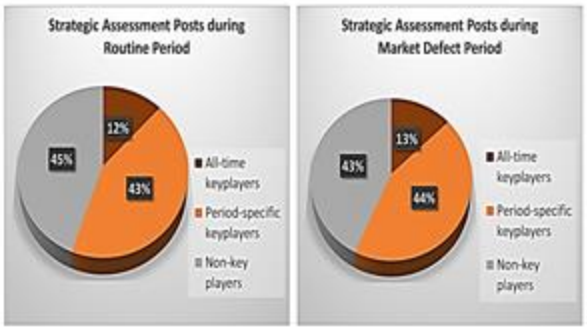

Figure 4. Percentage contribution of strategic knowledge sharing by types of users during routine vs. market defect period.

7. Conclusion

The current study investigated a subreddit forum for cryptomarket market activities on the dark web. We defined an online community of illicit market users as a form of community of practice. Although illicit market communities in the dark web are unique in that the nature of practice is concealed and illegitimate, they are ultimately human organizing system. By examining illicit market communities as self-organized knowledge-sharing collectives, this paper attempted to expand the understanding of the communicatively organizing principles for uncertainty management in illicit cyber-market system. Our results suggest that, despite the illicit nature, the collaborative dynamics and organizing principles were strikingly resonant with essential characteristics of "normal" communities of practice.

Particularly, this study focused on the comparison between routine and market defect periods. Literature on emergent collaboration networks has suggested that efficient network structures may vary depending on whether a task is routine and non-routine [28]. Drawn from early insights, this study compared the network structures as well as the content of strategic knowledge shared in each period.

Findings suggested that, while the distribution of sheer volume of strategic posts was not much different between the two periods, several differences were observed: (a) the network structure changed such that the network size grew while co-posting patterns were more centralized; (b) new crisis-specific key players emerged; (c) types of knowledge shared during the market defect period was qualitatively different from the routine period. While the majority of strategic knowledge was contributed by a small fraction of key players, the contribution by non-key players, who may also be defined as "peripheral legitimate participants" [27, p.1226], was not trivial. Future research is

recommended to examine how different or similar the nature of shared knowledge is between different user types (all-time key players, period-specific key players, and peripheral legitimate participants). The current study is one of early work on communication network evolution in hidden cyber collectives. While the findings and discussions in this paper are preliminary, future research may delve further into communication organizational principles in "normal" online communities and virtual organizations, and systematically compare how similar or different the illicit cyber-communities on the dark web are from the communities in visible digital space.

8. Acknowledgment

This research was sponsored by the Army Research Office and was accomplished under Grant Number W911NF-19-1-0066. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the Army Research Office or the U.S. Government. The U.S. Government is authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright notation herein.

9. References

[1] C. M. Chiu, M. H. Hsu, and E. T. Wang, "Understanding Knowledge Sharing in Virtual Communities: An Integration of Social Capital and Social Cognitive Theories", Decision Support Systems, Elsevier, Netherlands, 2006, pp. 1872-1888.

[2] A. Ardichvili, V. Page, and T. Wentling, "Motivation and Barriers to Participation in Virtual Knowledge-Sharing Communities of Practice", Journal of Knowledge Management, Emerald Publishing Limited, United Kingdom, 2003, pp. 64-77.

[3] M. Alsharo, D. Gregg, and R. Ramirez, "Virtual Team Effectiveness: The Role of Knowledge Sharing and Trust", Information & Management, Elsevier, Netherlands, 2017, pp. 479-490.

[4] P. Sarka, and C. Ipsen, "Knowledge Sharing via Social Media in Software Development: A Systematic Literature Review", Knowledge Management Research & Practice, Taylor & Francis, United Kingdom, 2017, pp. 594-609.

[5] B. Vasilescu, A. Serebrenik, P. Devanbu, and V. Filkov, "How Social Q&A Sites are Changing Knowledge Sharing in Open Source Software Communities", in Proceedings of the 17th ACM Conference on Computer Supported Cooperative Work & Social Computing, February 2014, pp. 342-354.

[6] I. Y. Chen, N. S. Chen, and Kinshuk, "Examining the Factors Influencing Participants' Knowledge Sharing Behavior in Virtual Learning Communities", Journal of Educational Technology & Society, National Taiwan Normal University, Taiwan, 2009, pp. 134-148.

[7] A. Halavais, K. H. Kwon, S. Havener, and J. Striker, "Badges of Friendship: Social Influence and Badge Acquisition on Stack Overflow", in 2014 47th Hawaii International Conference on System Sciences, Hawaii, January 2014, pp. 1607-1615.

[8] R. Yilmaz, "Knowledge Sharing Behaviors in E-Learning Community: Exploring the Role of Academic Self-Efficacy and Sense of Community", Computers in Human Behavior, Elsevier, Netherlands, 2016, pp. 373-382.

[9] J. Lave, and E. Wenger, Situated Learning: Legitimate Peripheral Participation, Cambridge University Press, United Kingdom, 1991.

[10] Barratt, M. J., and A. Maddox, "Active Engagement with Stigmatised Communities through Digital Ethnography", Qualitative Research, Emerald Publishing Limited, United Kingdom, 2016, pp. 701-719.

[11] R. W. Gehl, Weaving the Dark Web: Legitimacy on Freenet, Tor, and I2P, MIT Press, USA, 2018.

[12] R. W. Gehl, "Power/Freedom on the Dark Web: A Digital Ethnography of the Dark Web Social Network", New Media & Society, 2016, pp. 1219-1235.

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

[14] Department of Justice, "AlphaBay, the Largest Online 'Dark Market,' Shut Down", 2017, Retrieved from https://www.justice.gov/opa/pr/alphabay-largest-online-dark-market-shut-down

[15] K. Moeller, R. Munksgaard, and J. Demant, "Flow My FE the Vendor Said: Exploring Violent and Fraudulent Resource Exchanges on Cryptomarkets for Illicit Drugs", American Behavioral Scientist, SAGE Publishing, USA, 2017, pp. 1427-1450.

[16] M. C. Van Hout, and T. Bingham, "Responsible Vendors, Intelligent Consumers: Silk Road, the Online Revolution in Drug Trading", International Journal of Drug Policy, Elsevier, Netherlands, 2014, pp. 183-189.

[17] J. L. Schneider, "Hiding in Plain Sight: An Exploration of the Illegal(?) Activities of a Drugs Newsgroup", The Howard Journal, Wiley-Blackwell, USA, 2003, pp. 374-389.

[18] CourtListener.com, "U.S. vs Marc Peter Willems et. al." 2009, Retrieved from https://www.courtlistener.com/recap/gov.uscourts.cacd.518379.1.0.pdf

[19] E. Nunes, A. Diab, A. Gunn, E. Marin, V. Mishra, V. Paliath, ., ... and P. Shakarian, "Darknet and Deepnet Mining for Proactive Cybersecurity Threat Intelligence", in 2016 IEEE Conference on Intelligence and Security Informatics (ISI), IEEE, USA, September 2016, pp. 7-12.

[20] K. H. Kwon, and J. Shakarian, "Black-Hat Hackers' Crisis Information Processing in the Darknet: A Case Study of Cyber Underground Market Shutdowns", in Networks, Hacking, and Media–CITA MS@ 30: Now and Then and Tomorrow, Emerald Publishing Limited, United Kingdom, 2018, pp. 113-135.

[21] K. H. Kwon, J. H. Priniski, S. Sarkar, J. Shakarian, and P. Shakarian, "Crisis and Collective Problem Solving in Dark Web: An Exploration of a Black Hat Forum", in Proceedings of the 8th International Conference on Social Media & Society, USA, July 2017, p. 45.

[22] J. Shakarian, A. T. Gunn, and P. Shakarian, "Exploring Malicious Hacker Forums", in S. Jajodia, V. Subrahmanian, V. Swarup, and C. Wang, Cyber Deception, Springer Link, USA, 2016, pp. 259-282.

[23] N. Lin, Social capital: A theory of Social Structure and Action (Vol. 19), Cambridge University Press, United Kingdom, 2002.

[24] E. C. Wenger, and W. M. Snyder, "Communities of Practice: The Organizational Frontier", Harvard Business Review, 2000, pp. 139-146.

[25] E. Wenger, "Communities of Practice", Communities, Wenger-Trayner, USA, 2009.

[26] J. S. Brown, and P. Duguid, "Organizational Learning and Communities-of-Practice: Toward a Unified View of Working, Learning, and Innovation", Organization Science, The Institute for Operations Research and the Management Sciences (INFORMS), USA, 1991, pp. 40-57.

[27] S. Faraj, S. L. Jarvenpaa, and A. Majchrzak, "Knowledge Collaboration in Online Communities", Organization Science, The Institute for Operations Research and the Management Sciences (INFORMS), USA, 2011, pp. 1224-1239.

[28] M. K. Ahuja, and K. M. Carley, "Network Structure in Virtual Organizations", Organization Science, The Institute for Operations Research and the Management Sciences (INFORMS), USA, 1999, pp. 741-757.

[29] P. R. Monge, P. S. Contractor, and N. S. Contractor, Theories of Communication Networks, Oxford University Press, USA. 2003.

[30] N. S. Contractor, S. Wasserman, and K. Faust, "Testing Multitheoretical, Multilevel Hypotheses about Organizational Networks: An Analytic Framework and Empirical Example", Academy of Management Review, The Academy of Management (AOM; the Academy), USA, 2006, pp. 681-703.

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

[32] J.A. Danowski, and P. Edison-Swift, "Crisis Effects on Intraorganizational Computer-based Communication", Communication Research, USA, 1985, 12(2), pp. 251-270.

[33] X. Lu, and C. Brelsford, "Network Structure and Community Evolution on Twitter: Human Behavior Change in Response to the 2011 Japanese Earthquake and Tsunami", Scientific Reports, USA, 2014, 4, p. 6773.

[34] L. Palen, S. Vieweg, S.B. Liu, and A.L. Hughes, "Crisis in a networked world: Features of computer-mediated communication in the April 16, 2007, Virginia Tech event", Social Science Computer Review, 27(4), 2009, pp. 467-480.

[35] G. King, J. Pan, and M. E. Roberts, "How Censorship in China Allows Government Criticism but Silences Collective Expression", American Political Science Review, the American Political Science Association, USA, 2013, pp. 326-343.

[36] G. Grote, Management of Uncertainty: Theory and Application in the Design of Systems and Organizations, Springer Science & Business Media, Springer Nature, Germany, 2009.

[37] D. M. Webster, and A.W. Kruglanski, "Individual Differences in Need for Cognitive Closure", Journal of Personality and Social Psychology, The American Psychological Association (APA), USA, 1994, pp. 1049-1062.