Strategies to Disrupt Online Child Pornography Networks

Kila Joffres, Martin Bouchard, Richard Frank, Bryce Westlake
School of Criminology
International Cybercrime Research Centre
Simon Fraser University
Burnaby, Canada
{ kja4, mbouchard, rfrank, bwestlak }@sfu.ca

Abstract— **This paper seeks to determine which attack strategies (hub, bridge, or fragmentation) are most effective at disrupting two online child pornography networks in terms of outcome measures that include density, clustering, compactness, and average path length. For this purpose, two networks were extracted using a web-crawler that recursively follows child exploitation sites. It was found that different attack strategies were warranted depending on the outcome measure and the network structure. Overall, hub attacks were most effective at reducing network density and clustering, whereas fragmentation attacks were most effective at reducing the network's distance-based cohesion and average path length. In certain cases, bridge attacks were almost as effective as some of these measures.**

Keywords- Social network analysis, Child exploitation, Network disruption, Internet

I. Introduction

As early as the 18th century, academics have been interested in networks as purely theoretical objects [1]. Networks have since emerged as a practical tool for representing real world systems of interacting components, ranging from the Internet to biological structures. This paper examines the most effective measures of disrupting child pornography networks situated on the World Wide Web. The Web, as a network of sites connected by hyperlinks, has transformed the manner in which people access and distribute information. In doing so, it has attracted considerable worldwide popularity; however, it has also produced certain unintended consequences. This is particularly the case for child pornography, where the Internet's apparent anonymity, global reach, and lack of regulation have rendered it a popular, easy, and effective outlet for distributing and accessing such illegal materials [2] [3]. The extent of this issue was recently emphasized by the United Nations, which estimated that over four million websites featured child pornography [4].

Current attempts to limit child exploitation have often focused on chat room stings, injunctions against websites hosting child pornography, establishing hotlines and complaint sites, and image databases [5] [6]. While these efforts have, to some extent, impeded the spread and access of child pornography, they are not necessarily the most effective means of doing so. Specifically, two problems arise from such intervention strategies. First, there tends to be an overreliance on investigating and targeting sites in isolation. As a more effective approach, some argue that law enforcement should focus on the links between sites and the reliance of individuals on these networks [7]. This approach acknowledges that the connections between child pornography sites, and the networks they form, are important to consumers, and as such, they are a valuable focus for intervention. Second, current enforcement efforts have been met with limited success. For instance, it is estimated that less than 1% of online pedophiles are caught [8].

There is a clear need for more effective strategies for disrupting online child pornography sites. This can be achieved through a networks perspective, which has demonstrated its usefulness in identifying successful attack strategies for various networks, including the Internet and child exploitation sites [9] [10]. In identifying appropriate attack strategies, it is important to consider the topology of the networks [11] [12]. Online networks have two important structural features: they tend to follow a power-law distribution and demonstrate small-world properties. On account of its power-law properties, the Web is characterized by: (a) many websites with few links and (b) a few sites with many links [13] [14] [9] [15]. That is, the Web is distinguished by a few very highly connected nodes, or hubs, which fundamentally define the network's topology. Hence, the Web is described as following a power-law expression with a scale-free distribution. Furthermore, the Web has been found to demonstrate small-world characteristics. Despite its vast size (several billion documents), the average path length within the Web generally ranges from 16 to 19 [16] [17]. Additional work by Stanford University has indicated that there is a high degree of clustering in the Web; that is, the likelihood that two sites, which are connected to a common neighbour, are also linked to one another is much greater than expected from a random network [17]. This finding has been extended to online networks with illegal content. For instance, [12] found small-world characteristics in an online terrorist network.

The topology of networks has specific implications for law enforcement strategies. Research comparing the effectiveness of random attacks versus targeted attacks on scale-free networks has found that such networks are resilient to the former and vulnerable to the latter [14] [18] [12]. Because poorly linked nodes in scale-free networks appear more frequently, they will be disproportionately affected by random attacks. Given that the contribution of these nodes to the integrity of the network is relatively insignificant, the network often remains connected [9]. As a result, random attacks tend to be less effective. However, the robustness of scale-free networks comes at a cost: repeated attacks targeted at the hubs can effectively disconnect a network [14].

In their work, [11] also studied which law enforcement strategies worked best for certain network structures. They found that the extent to which a network demonstrates small-world characteristics (e.g., an average of 6 paths separating nodes), scale-free properties (e.g., contains hubs in which a node had many connections), and vulnerability features (e.g., high fragmentation scores) affected which targeting strategies were best (e.g., a hub attack, a repeated hub attack, a bridge attack, or a combination thereof). For example, with small-world networks, which have high levels of clustering and thus leave nodes in a position to replace others, repeated attacks on multiple nodes will most successfully disrupt the network [11]. In contrast, scale-free networks will be best disrupted through hub attacks [14] [19] [12]. Finally, networks with high vulnerability, characterized by many actors who bridge together subgroups, will be susceptible to attacks that disrupt these bridges, thereby severing the flow of information [8] [11]. In another study, [12] found that pure scale-free networks were vulnerable to both hub and bridge attacks, while small-world networks were more vulnerable to bridge attacks.

[13] [11] [12] introduced broad strategies for attacking networks. These strategies identify nodes with a particular type of centrality in the network, each amenable to specific suggestions for targeting key players. Diverse measures of centrality have been examined in the literature, the most common including measures of degree (the number of ties a node has) and betweenness (the extent to which a node brokers between others) [20] [22]. Hub attacks target those nodes with many links to and from other nodes in a network. In this sense, hub attacks remove those nodes high in degree centrality. Conversely, bridge attacks sever those nodes that connect other nodes in a network, those high in betweenness centrality.

Degree centrality and betweenness centrality have previously been described as useful measures to identify prominent nodes [23] [24] [25] [26]. However, identifying key players to target in a network is not necessarily obvious. For example, [27] argues that traditional measures of centrality cannot "optimally solve the key player problem" (p. 127). It is possible for traditional measures to identify a node that, while central in a network, will cause little disruption if removed. This would occur if, for example, a node is linked to many actors, but these actors can still reach each other through alternative ties when this central node is removed. Conversely, if many actors in a network rely on a particular node to reach each other, its removal would have a more significant impact on the network. Instead of being redundant, this node is integral to the flow of information in the network, making it a valuable law enforcement target. To resolve the problem of redundancy, [27] develops the measure of fragmentation to identify those actors whose removal would most disrupt the network.

Thus, this paper examines three attack strategies identified as important in the literature in order to determine which will produce the greatest disruption in two different online child pornography networks[1]. These strategies include hub attacks (target nodes with high degree centrality), bridge attacks (target nodes with high betweenness) and fragmentation attacks (target nodes whose removal would sever the greatest number of connections). This will allow us to select the strategy that will cause the largest disruption to the child pornography networks while expending the least amount of resources.

II. Methods

To evaluate different strategies of disrupting child exploitation networks, the method presented in this paper first extracts a sub-network, which deals with child exploitation material, from the Web (Section A), and then uses established SNA tools to guide attacks against the network (Section B).

A. *The Child Exploitation Network Extractor (CENE)*

Two online networks were used in this project; they were produced using a custom-written web-crawler called the Child Exploitation Network Extractor (CENE) [10]. The algorithm for CENE is located in Figure 1. This crawler is designed to recursively follow links from a starting website until it meets specific termination criteria (i.e., a certain number of pages and websites). As the crawler does this, it collects statistics on the number of keywords, images and videos on each of the webpages stemming from that particular website. This information is then aggregated at the website level. The product is a mapped network of websites with information on the content within, and the directed links between, these websites.

Three limits were imposed on CENE to prevent it from perpetually crawling the Internet. First, a limit of 250,000 webpages retrieved was included to keep the extraction process time bounded. Second, network size was limited to 200 websites, with webpages sampled as equally as possible between websites. Third, a set of keywords were defined in an attempt to ensure that the websites extracted were topic relevant. This set includes 63 child pornography related words, many of which were (a) commonly used by the Royal Canadian Mounted Police (RCMP) to locate illegal child-related content and (b) used in other studies of online child pornography [28]. The web-crawler included 'softcore' words such as girl, boy, love, child, teen, variations of Lolita, young, bath*, twink, pre/post pubescent, innocent, smooth and hairless. It also included a set of 'hardcore' words, such as penis, cock, vagina, pussy, anus, anal, sex, pedo/paedo, oral, virgin, naked and nude.

To be included into the network, a webpage had to have at least seven of the 63 keywords. If it failed to meet this criterion, the webpage was discarded and no links were followed from it. It was determined through manual verification that seven keywords reliably distinguished between child exploitation webpages and unrelated ones. The web-crawler also discarded broken links or websites inaccessible for other reasons (including timeouts or password barriers). Videos and images from each webpage were also recorded. In order to avoid including very small images such as logos and

[1] Other potential key player measures were examined, including Bonacich centrality, Freeman closeness, point connectivity, and cutpoints. However, they did not emerge as important disruption measures.

```
Algorithm CENE(StartPage, PageLimit, WebsiteLimit, Keywords(), BadWebsites(), minImageWidth, minImageHeight)
    $Queue() \leftarrow \{StartPage\}$
    $KeywordsInWebsiteCounter() \leftarrow 0$, $LinkFrequency() \leftarrow \{\}$, $WebsitesUsed() \leftarrow \{\}$, $FollowedLinks() \leftarrow \{\}$
        //initialize variables
    while $|FollowedPages| < PageLimit$ and $|Queue| > 0$
        $P \leftarrow Queue(1)$, $D_P \leftarrow$ domain of $P$          //start evaluating next page in queue
        if $D_P \notin WebsitesUsed()$ and $|WebsitesUsed| < WebsiteLimit$ then
            $WebsitesUsed() \leftarrow WebsitesUsed() + D_P$
        if $D_P \in WebsitesUsed()$ and $D_P \notin BadWebsites()$ then          //evaluate this page
            $PageContents \leftarrow$ Retrieve page $P$
            $VideoCounter \leftarrow 0$, $ImageCounter \leftarrow 0$
            $FollowedPages \leftarrow FollowedPages + P$
            if $PageContents$ contains $Keywords()$
                $KeywordsInWebsiteCounter() \leftarrow$ get frequency of all $Keywords()$
                $LinksToFollow() \leftarrow$ all {href} elements in $PageContents$
                for each $L$ in $LinksToFollow()$
                    if $L$ links to an image
                        $ImageContents \leftarrow$ retrieve image $I$          //if the link leads to an image
                        If width(ImageContents) > minImageWidth and height(ImageContents) > minImageHeight then
                            $ImageCounter \leftarrow ImageCounter + 1$          //count only if the image is big enough
                    elseif $L$ links to a video          //if the link leads to a video
                        $VideoCounter \leftarrow VideoCounter + 1$
                    elseif $L \notin Queue()$ and $L \notin FollowedPages$
                        $Queue() \leftarrow Queue() + L$
                        $D_L \leftarrow$ domain of $L$
                        $LinkFrequency(D_P, D_L) \leftarrow LinkFrequency(D_P, D_L) + 1$
                $VideosInWebsite(D_P) \leftarrow VideosInWebsite(D_P) + VideoCounter$
                $ImagesInWebsite(D_P) \leftarrow ImagesInWebsite(D_P) + ImageCounter$
                $KeywordsInWebsite(D_P) \leftarrow KeywordsInWebsite(D_P) + KeywordsInWebsiteCounter()$
    return WebsitesUsed(), KeywordsInWebsite(), LinkFrequency(), VideosInWebsite(), ImagesInWebsite()
```

Figure 1. Algorithm CENE

emoticons, images were recorded only if they were 150x150 pixels or larger. No requirement was imposed on videos.

For this study, two networks were extracted using different starting websites, one referred to as Network A and another as Network B. Network A was identified as girl-centered, where more than half of the keywords on websites included female-related terms such as vagina Lolita, girl, and so on. Network B was boy-centered, with websites including mostly male-related terms as penis and boy. Given the keyword requirements, these networks were expected to include websites or blogs with child pornography or other child exploitative materials.

While CENE provides a useful way of uncovering online child pornography networks, it is not without limitations. For instance, given the nature of some of the keywords, there is the possibility of false positives (for example, it is possible for a website to include words such as child, girl, boy, young, teen, and innocent, and not be about child exploitation). Nonetheless, these websites may link to child pornography or vice-versa. In this way, they play a role in the network that may also be relevant to examine. A further limitation of the web-crawler is its inability to analyze content from, and follow links out of, password protected websites. Consequently, these websites were not captured in the networks. Nonetheless, CENE remains a helpful method for extracting networks of child exploitation websites.

B. Social Network Measures

This paper seeks to identify the most effective social network analysis measures to disrupt online child pornography networks. For this purpose, various attack strategies were used to identify particular sites whose elimination would have the largest impact on specific outcome measures. These attack strategies involve hub attacks (using the measure of degree centrality), bridge attacks (using the measure of betweenness), fragmentation attacks (using the measure developed by [27]), and random attacks (where each node has an equal chance of being targeted).

With the exception of random attacks, each of these network disruption strategies identifies key players who are central to the network in varying ways. For hub attacks, the degree centrality measure examines the number of ties that a node website has to other websites. The underlying assumption of this measure is that nodes with many connections are more likely to be powerful since they can directly influence more actors, access more resources in a network, and are less dependent on other actors since they have alternative means for fulfilling their needs [29]. Our networks have directed ties; some websites link to others (out-degree ties) while some websites are linked to by others (in-degree ties). Websites with many in-degree ties may be considered more important or prominent; a website can easily link to others, but it may not be relevant or interesting enough to receive links from other websites. By virtue of their ability to attract traffic, popular sites may be important law enforcement targets. Websites with out-degree ties are also valuable to consumers, as they may connect them with many other websites, thus providing them with abundant access to materials in the network.

For bridge attacks, betweenness centrality identifies those websites that fall on the shortest path between other websites in a network [29]. It describes the extent to which a website 'brokers' between other websites. In a network, this position can be advantageous, as it allows certain websites to bridge groups and control the flow of information between actors [11]. For interested individuals, these websites are important insofar as they provide access to various parts of a child pornography network that would otherwise be more difficult to reach.

Key players were also identified through a fragmentation analysis. This measure indicates the proportion of sites that would not be able to reach each other if any particular site was removed [27]. This produces disconnections in the network that would limit an individual's ability access to other websites.

The removal of websites identified by these measures followed a sequential process which involved (a) identifying the website that scored highest for one measure, (b) removing it, and (c) reanalyzing the network to identify the next top website. This process was repeated until five websites were eliminated. This strategy avoids the potentially redundant effect of eliminating certain websites simultaneously [27] [12] [30].

The impact of removing the five websites that scored highest on the three centrality measures was then examined on several outcome measures. The first outcome measure included is network density. Density is calculated by dividing the number of existing ties in a network with the number of possible ties [29]. Assessing the changes in density is valuable, since it examines the changes in the amount of ties. The more ties that are eliminated in a network, the more difficult it is for individuals to reach other websites. Change in the overall clustering of the network was also assessed. The clustering coefficient is the average density of the neighbourhoods of the websites in a network [29]. In other words, it examines the likelihood that two websites, which are linked to one particular website, are also linked to one another. As with the overall network density, by eliminating certain websites, and therefore certain ties within a cluster or a neighbourhood, access to materials within a network becomes more difficult. In addition, this prevents consumers from becoming embedded in a tightly-knit community that promotes their views and interests.

Finally, two measures of network cohesion were examined: distance between pairs and distance-based cohesiveness. The distance between pairs examines the average number of paths required for a site to reach other websites in the network [29]. For the purposes of this paper, a measure that produces the greatest reduction in this measure is sought. While this may seem counterintuitive, it is important to note that this measure only calculates the distance between reachable nodes. As such, a drop in the average path length in a network after an attack can be attributed to the fact that fewer websites are now reachable. Conversely, distance-based cohesiveness represents the extent to which a network is compact (i.e., overall, how close websites are to each other). Again, greater cohesiveness suggests a better flow of information and more linkages between websites in a network; consequently, a decrease in this measure would further impede an individual's efforts to easily reach child pornography.

TABLE I. NETWORK DESCRIPTIVES

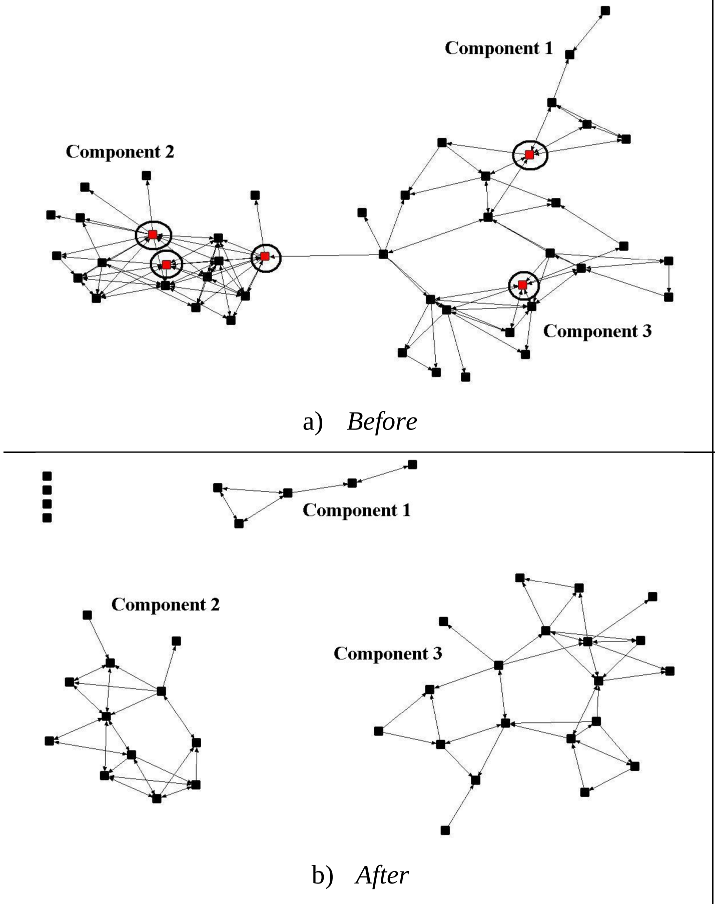
Measure		Network			
		Network A	Random Network A	Network B	Random Network B
Nodes		46	46	111	111
Ties		150	150	663	663
Density		0.0725	0.0725	0.0543	0.0543
Clustering Coefficient		0.442	0.083	0.424	0.056
Average Path Length		3.49	3.172	2.409	2.809
Distance-Based Cohesion		0.200	0.354	0.131	0.398
Centra-lization	Out	19.852%	10.765%	21.124%	5.562%
	In	13.037%	10.765%	22.041%	9.231%

III. Results

A. Descriptive Features

The structure of both networks was first assessed. Network A had a total of 46 nodes and 150 ties, while Network B had 111 nodes and 663 ties (table 1). The difference in size exists because that web-crawler visited all links outside of a website and subsequently analyzed its content to determine whether or not it would be included in the network. If the website did not meet the necessary criteria, it was not included in the network; however, it still counted in terms of 200 website limit imposed on the web-crawler. For example, in Network A, 154 websites were considered irrelevant while 46 were found relevant.

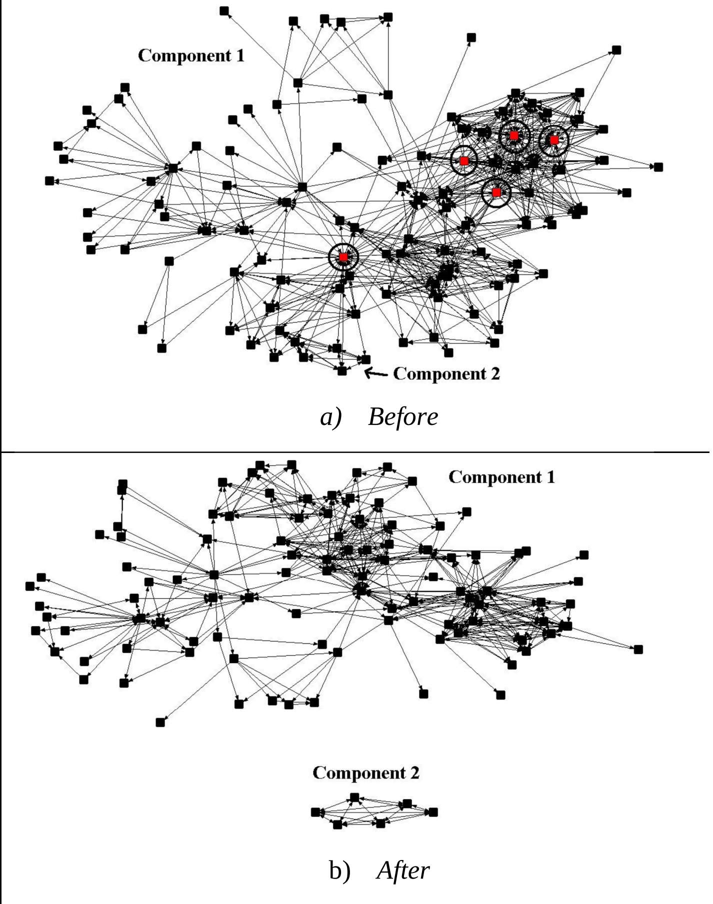
When examining the network structure, Network A had a higher density than Network B (0.073 vs. 0.054), a higher clustering coefficient (0.442 vs. 0.424) and a higher average path length (3.490 vs. 2.409). However, Network B demonstrated greater compactness (0.200 compared to 0.131 for Network A). Thus, although there is more information (i.e., websites) available Network B, this information was more difficult to access, given that fewer links exist between websites. The centralization of the networks was also examined; this measure expresses the overall degree of variance in network centrality as a percentage [29]. Both networks had similar out-degree centralization (approximately twenty percent for Network A and twenty-one percent for Network B), but differed largely in terms of in-degree centralization (approximately thirteen percent and twenty-two percent respectively). This demonstrates some concentration of



a) *Before*

b) *After*

Figure 2. Network A before and after Out-Degree Attack



a) *Before*

b) *After*

Figure 3. Network B before and after Out-Degree Attack

out-going and in-going links within certain nodes in the networks. The exception is with Network A's in-degree centralization; there were fewer websites that dominate in terms of receiving links.

Both networks tend to display small world characteristics. For instance, both had an average path length shorter than the six, which is considered characteristic of small worlds [31]. In addition, both child pornography networks had higher (more) clustering than randomly generated networks, though these were more compact than the child pornography networks. Network A had a compactness or distance-based cohesion score of 0.200, whereas the random network had a score of 0.354. However, for clustering, Network A scored 0.442, which was much larger than the random network's score of 0.083. Similarly, Network B had a compactness score of 0.131, whereas the random network had one of 0.398. With respect to clustering, Network B scored 0.424, while the random network scored 0.056. The small average path length and relatively high degree of clustering are characteristic of small worlds.

Network A and Network B also had features seen in scale-free networks. For example, the networks showed greater centralization than the random ones (safe in the case of Network A's in-degree centralization, where the difference was more modest). For example, Network B had an in- and out-degree centralization of around twenty-one percent, which was more than double that of the random network. This indicates that Network A and Network B have more hubs than would be expected from a random network; a property identified in networks following a power-law distribution.

B. Density

For both Network A and Network B, the most effective strategy to reduce network density was to target those (five) websites with the highest degree centrality (i.e., to perform hub attacks) (see table 2). For Network A, the density fell from 0.0725 to 0.0500 for the out-degree measure while the number of ties dropped from 150 to 82. When the websites with the highest number of in-degree ties were removed, density fell to 0.0506 with 83 ties left. It is worth noting that removing websites that scored highest in betweenness, had the same impact as removing websites with the most in-degree ties. Thus, for Network A, both hub and bridge attacks were similarly effective. To illustrate the sequence of events, figure 3 shows the before and after process by which the original network is changed when the websites highest in out-degree scores are removed (circled in the figure). Most of the targeted websites are located in the hub to the right of the original network; in addition, as seen in graph b), the network is now fragmented into three separated components with four isolates.

Hub attacks were also most effective for Network B. Removing websites with the most out-degree ties produced the largest reduction in network density (0.0543 to 0.0442). The number of ties fell from 663 to 492. The original and resulting

TABLE II. DENSITY

Measure		Network A		Network B	
		Density (Change)	Ties Left	Density (Change)	Ties Left
Fragmentation		0.0561 (↓22.62%)	92	0.0482 (↓11.233%)	537
Betweenness		0.0506 (↓30.207%)	83	0.0469 (↓13.627%)	522
Degree	Out	0.0500 (↓31.034%)	82	0.0442 (↓18.6%)	492
	In	0.0506 (↓30.207%)	83	0.0455 (↓16.206%)	506
Random Attack		0.0732 (↑0.551%)	120	0.0541 (↓0.368%)	602

networks are shown in figure 4. It can be seen from graph b) that the network was fragmented into two separate components following the attack. The in-degree measure was relatively less effective at reducing density (though more effective than other measures). The density fell to 0.0455 with 506 ties remaining. This suggests that a more nuanced approach to hub attacks may be useful in certain cases.

As for random attacks, the density almost did not change for any of the two networks. This made it the least effective strategy for decreasing network density.

Note that hub attacks against Network A produced more disruption than the same attacks against Network B. For instance the out-degree attack on Network A created a 38.76% reduction in density, whereas this attack only produced an 18.60% reduction in Network B's density. Network size best explains this finding, as the removal of 5 nodes in smaller network A had a larger effect than for a network more than double its size.

C. Clustering Coefficient

In terms of reducing the clustering coefficient, degree centrality measures were once again the most effective strategy (see table 3). However, differences between the two networks emerged: for Network A, removing the five websites that scored highest for in-degree ties was the most effective strategy whereas removing the five websites with the highest out-degree scores was most successful in Network B.

When removing nodes with the highest in-degree scores, the clustering in Network A fell by 6.108% (to 0.415). Removing websites high in out-degree ties was half as effective, with the clustering coefficient dropping by 2.941% (to 0.429). For the Network B network, the only measure to reduce clustering was the out-degree one; all other measures slightly increased network clustering. This may be due to the removal of nodes with weak ties and relatively large distances from other nodes. When websites with the most outgoing links were removed from the network, the clustering coefficient dropped from 0.424 to 0.422 (0.471%). Again, these findings indicate that, in a directed network, it may be important to differentiate between in-degree and out-degree hub attacks. When the networks were attacked randomly, a small 0.001 reduction in the clustering coefficient was produced in Network A, whereas the clustering in Network B increased by 0.800.

TABLE III. OVERALL CLUSTERING COEFFICIENT

Measure		Network A	Network B
Fragmentation		0.514 (↑16.289%)	0.430 (↑1.415%)
Betweenness		0.438 (↓0.09%)	0.426 (↑0.471%)
Degree	Out	0.429 (↓2.941%)	0.422 (↓0.471%)
	In	0.415 (↓6.108%)	0.434 (↑2.358%)
Random Attack		0.441 (↓0.226%)	0.432 (↑1.886%)

Between networks, Network A was once again more easily disrupted by the hub attacks. The clustering fell by 6.108% in Network A, whereas it decreased by 0.471% in Network B. Furthermore, most measures in Network B actually increased clustering and the only measure to decrease it had a modest impact of 0.471%. This suggests that certain changes to Network B are prone to leaving it with more tightly-knit groups.

D. Distance-Based Cohesion and Average Path Length

Differences between networks also emerged for which measure produced the largest reduction in distance-based cohesion (see table 4). For Network A, targeting websites with the highest betweenness scores resulted in the largest decrease of cohesion (0.131 to 0.085). In this sense, a bridge attack was the most successful attack strategy. In contrast, for Network B, the fragmentation measure was the most effective, reducing cohesion from 0.200 to 0.073. For Network A, random attacks increased compactness from 0.200 to 0.207, whereas compactness was decreased from 0.131 to 0.129 in Network B. For Network A, this is the only attack that increased the network's cohesion; it is likely that distant, poorly connected websites were targeted by the random attack.

When the networks are compared, it can be seen that the fragmentation attack against Network B was more successful at reducing cohesion than Network A's bridge attack. In Network B, the network's compactness fell by 63.50%, whereas in Network A, it decreased by 35.11%. Notably, Network B' network was initially far more compact than Network A, with a distance-based cohesion of 0.200 compared to 0.131 for Network A. Thus, differences are more easily seen when Network B' network is fragmented.

As for the average path length, the fragmentation analysis produced the greatest reduction in the measure for both networks (see table 5). A reduction in this measure is desired on account of its implications: when the average path length decreases, it is only because fewer nodes have become reachable in the network. For Network A, the average path length decreased from 3.49 to 1.85, while the number of paths in the network fell from 1021 to 230. In contrast, a random attack increased the path length to 3.57; while this has the effect of increasing the time to reach other websites, more of these websites are still reachable (that is, 859 possible paths remained). In the fragmentation analysis for Network B, the average path length fell from 2.409 to 1.741, while the number of paths dropped from 1447 to 1164. Conversely, random attacks increased the path length to 2.414, with 2752 paths remaining. Again, random attacks were far less effective than targeted ones.

TABLE IV. DISTANCE-BASED COHESION

		Network	
Measure		Network A	Network B
Fragmentation		0.093 (↓29.007%)	0.073 (↓63.50%)
Betweenness		0.085 (↓35.114%)	0.075 (↓62.50%)
Degree	Out	0.103 (↓21.374%)	0.082 (↓59.0%)
	In	0.119 (↓9.16%)	0.434 (↑117.0%)
Random Attack		0.207 (↑58.015%)	0.129 (↓35.50%)

Furthermore, the fragmentation attack was particularly effective for Network A; the average path length decreased by 46.934% compared to 27.729% for Network B. The path length was initially larger for Network A (3.49) than Network B (2.41), indicating that more pathways between websites existed in the Network A network. Yet, given Network A's smaller network, the elimination of key websites would likely be more devastating to this network's structure.

IV. DISCUSSION

The purpose of this paper was to isolate those attack strategies (hub, bridge, fragmentation) that would maximally disrupt two online child exploitation networks. In doing so, this study extends past research on disruption strategies [27] [12]. Two online networks were used: a smaller girl-centered one (Network A) and a larger boy-centered one (Network B). Both of these were extracted using CENE, a web-crawler tailored to follow the links out of and into child exploitation websites when given a specific starting website. Three general findings emerged: (1) targeted attacks are more effective than random ones; (2) for different outcome measures (density, clustering, distance), different intervention strategies are warranted, and (3) for different networks, different attack strategies are more or less effective. As predicted by [14] randomly removing websites failed to produce as much damage to the networks as targeted attacks. Furthermore, the effectiveness of various types of targeted attacks (hub, bridge, or fragmentation) varied according to different law enforcement goals (reducing density, clustering, reachability or cohesion).

When the goal is to eliminate as many ties as possible in a network (i.e., reduce density) and/or to reduce a node's embeddedness in a tight-knit component of the network (clustering), hub attacks are the most effective strategy overall. This type of attack removes nodes high in degree centrality, which impedes an individual's ability to access websites in a network, as the links between them has been eliminated. [11] [19] [12] have also stressed the importance of hub attacks, identifying them as useful strategies for disrupting small-world and scale-free networks similar to Networks A and B. The current research extends this discussion by specifying for which outcome measures hub attacks are effective (i.e., density and clustering). Hub attacks may not benefit scale-free, small-world networks for other outcome measures. Instead, different attack strategies may be suitable. For example, [27] introduced the fragmentation measure, which was found to be more successful at reducing reachability within a network. As such, knowledge of the underlying network structure is not necessarily sufficient for selecting appropriate attack strategies; the end goal or outcome measure is also relevant.

TABLE V. AVERAGE PATH LENGTH

		Network	
Measure		Network A	Network B
Fragmentation		1.852 (↓46.934%)	1.741 (↓27.729%)
Betweenness		2.014 (↓42.292%)	1.812 (↓24.782%)
Degree	Out	2.738 (↓21.547%)	1.980 (↓17.808%)
	In	3.431 (↓1.69%)	2.049 (↓14.943%)
Random Attack		3.574 (↑2.406%)	2.414 (↑0.207%)

Nonetheless, the network structure remains important. [11] [19] [12] have recognized that differences in network structure produce variation in the effectiveness of certain attacks. However, there is great diversity and complexity between and within networks, the implications of which have not necessarily been teased out by these researchers. For example, within networks, it may be important to differentiate between in-degree and out-degree hub attacks, as one approach may be more effective than the other. The direction of these links has certain implications in terms of network disruption. By eliminating websites that others link to the most often (in-degree), potentially relevant and important websites have been removed from the network. In contrast, by eliminating websites that are prolific linkers (out-degree), an individual's ability to spread through the network is inhibited. It is also possible for a network to have more than one effective attack strategy. For instance, both hub and bridge attacks were similarly effective at reducing density in Network A because some of the same nodes were targeted. Targeting websites high in betweenness can also be a valuable strategy, as this eliminates the bridges between websites, thereby impeding a person's exposure to diverse child pornography materials and potentially constraining him or her to small parts of a network.

In addition, certain network structures appear to be easier to disrupt; for instance, attacks against the smaller, denser Network A generally had a greater impact than those on the larger Network B. [11] indicated that, for small world networks, repeated attacks were necessary to maximize disruption; this was indeed the case for Network B, the larger, more compact network with a shorter average path length. For such networks as Network A, fewer resources may need to be expended to satisfactorily destroy the network. In essence, this study found that it is important not only to consider the desired outcome for an attack, but also the particular network structure being attacked. This leads to a more nuanced approach to network attacks.

There are several limitations to this study. As previously mentioned, it is possible for the networks to include false positives; i.e., websites that do not involve child exploitation. This is difficult to avoid; however, attempts to minimize false positives were made with the seven keywords requirement. Furthermore, given that these websites link to or from child pornography, they arguably remain, to some extent, relevant to the network structure. The small size of the networks is also problematic considering the millions of available child pornography websites. As such, the networks used may represent only a mere fraction of a more complete network. Limitations to the web-crawler may also have inhibited the extraction of complete networks. For instance, it is possible that some of the most relevant or severe child pornography websites were password protected; this would prevent CENE from accessing them and as such, they (and the websites they link to) would not be included in the network.

V. Conclusions

This project sought to determine which attack strategies would most successfully disrupt online child pornography networks. These networks were extracted using CENE, a web-crawler designed to follow, and gather information on, child exploitation websites. It was found that the most effective attack strategies depend on both (a) the specific law enforcement goals or outcome measures and (b) the particular structure of the network.

This has practical implications in terms of focusing the effective use of police resources and decreasing the accessibility of online child pornography. Pairing the web-crawler with social network analyses help target prioritization by identifying websites that would maximally disrupt the network given its structure and the desired outcomes. This would most effectively limit an individual's ability to travel through networks and access increasing amounts of child pornography. The current study provides methodological guidelines on which to base such decisions.

Future work should adopt longitudinal designs. Tracking the way networks evolve as specific nodes are attacked and removed from it should be a priority. Within the context of the current study, monitoring changes in site linkage behavior would provide a promising start point for such research. It is also possible that certain networks recover from, or adapt more easily to, specific attacks [32]. In addition, the manner in which a network reacts to changes may create a new context that modifies which attack strategy is most effective. This type of research can also be extended to other types of illicit or "dark" networks online. With some modifications to the web-crawler, networks of websites that promote terrorism, drug use, or other illegal behavior can be extracted. This allows for the replication and extension of the results of the current study.

VI. References

1) M.E.J. Newman, "The physics of networks," Phys. Tod., vol. 61, pp. 31-33, February 2008.

2) A. Spink, H.C. Ozmutlu, and D.P. Lorence, "Web searching for sexual information: An exploratory study," Info. Process. and Manag.: An Intern. Journ., vol. 40, pp. 113-123, January 2004.

3) K.S. Young, and E. Griffin-Shelley, A. Cooper, J. O'Mara, and J. Buchanan, "Online infidelity: A new dimension in couple relationships with implications for evaluation and treatment," in The Dark Side of the Force, A. Cooper, Ed. Philadelphia: Brunner Routledge, 2000, pp. 59-74.

4) E. Engeler, "E. UN expert: Child porn on internet increases. The Associated Press," September 2009. Retrieved from http://www.msnbc.msn.com/id/32880508/ns/technology_and_science-security

5) J. Stanley, "Child abuse and the Internet," Chil.. Abu. Prev. Iss., vol. 15, pp. 1-20, 2001.

6) R. Wortley, and S. Smallbone. Child Pornography on the Internet. Washington, DC: Office of Community Oriented Policing Services, 2006.

7) T. Krone, "A typology of online child pornography offending," Tren. and Iss. in Crim. and Crim. Just., vol. 279, pp. 1-6, July 2004.

8) J. McLaughlin, "Cyber child sex offender typology", 2004. Available at: http://www.ci.keen.nh.us/police/typology.html

9) A.-L. Barabási, Linked: How Everything is Connected to Everything Else and What it Means for Business, Science, and Everyday Life. New York: Penguin Group, 2003.

10) R. Frank, B. Westlake, and M. Bouchard, "The structure and content of online child exploitation networks," Proceedings of the tenth ACM SIGKDD Workshop on Intelligence and Security Informatics, 2010.

11) A. Malm, and G. Bichler, "Networks of collaborating criminals: Assessing the structural vulnerability of drug markets," J. of Res. in Crim. and Del., vol. 00, pp. 1-25, 2011.

12) J. Xu, and H. Chen, "The topology of dark networks," Comm. of the ACM, vol. 51, pp. 58-65, October 2008.

13) L.A., Adamic, and B.A. Huberman, "Power-law distribution of the World Wide Web," Science, vol. 287, pp. 2115a, February 2000.

14) R. Albert, H. Jeong, and A.-L. Barabási, "Attack and error tolerance of complex networks," Nature, vol. 406, pp. 378-382, July 2000.

15) R. Kumar, S. Rajalopagan, and A. Tomkins, "Extracting large-scale knowledge bases from the web," Proceedings of the 9th ACM Symposium on Principles of Database Systems 1, 1990.

16) L.A., Adamic, "The small world web," in Proceedings of the 3rd European Conf. on Digital Libraries, S. Abiteboul, and A.-M, Vercoustre, Eds. Berlin: Springer-Verlag, 1999, pp. 443-452.

17) A.-L. Barabási, "The physics of the Web," Physics World, vol. 14, pp. 33-38, July 2001.

18) C. Labovitz, A. Ahuja, and F. Jahanian, "Delayed Internet routing convergence," Proceedings of Institute of Electrical and Electronics Engineers (IEEE) Symposium on Fault-Tolerant Computing STCS, June 1999.

19) R. Medina, and G. Hepner, "Geospatial analysis of dynamic terrorist networks," in Values and Violence: Intangible Aspects of Terrorism, I. Karawan, W. McCormack and S.E. Reynolds, Eds. Berlin, Germany: Springer, 2008, pp. 151-167.

20) J. McGloin, "Policy and intervention considerations of a network analysis of street gangs," Crim. and Pub. Pol., vol. 4, pp. 607-636, August 2005.

21) L.C. Freeman, "Centrality in social networks conceptual clarification. Social Network", Soc. Net., vol. 1, pp. 215-239, 1978/9.

22) S. Wasserman, and K. Faust, K, Social Network Analysis: Methods and Applications. Cambridge, UK: Cambridge University Press, 1994.

23) W.E. Baker, and R.R. Faulkner, "The social organization of conspiracy: Illegal networks in the heavy electrical equipment industry," Amer. Soc. Rev., vol. 58, pp. 837-860, December1993.

24) V.E. Krebs, "Mapping networks of terrorist cells," Connections, vol. 24, pp. 43-52, 2002.

25) R.S. Burt, Structural Holes. Cambridge, MA: Harvard University Press, 1992.

26) C. Morselli, and P. Tremblay, "Criminal achievement, offender networks, and the benefits of low self-control,". Criminology, vol. 42, pp. 773-804, August 2004.

27) S. Borgatti, "The key player problem," in Dynamic Social Network Modeling and Analysis: Workshop Summary and Papers, R. Breiger, K. Carley, and P. Pattison, Eds. Washington D.C.: National Academy of Science Press, 2003, pp. 241-252.

28) B. Le Grand, J. Guillaume, M. Latapy, and C. Magnien, "Dynamics of paedophile keywords in eDonkey queries: Measurements and analysis of P2P activity against paedophile content project", 2009. Retrieved from: http://antipaedo.lip6.fr/

29) R. Hanneman, and M. Riddle, Introduction to Social Network Methods. Riverside, CA: University of California, Riverside, 2005.

30) D.M. Schwartz, and T. Rouselle, "Using social network analysis to target criminal networks," Tren. in Org. Crim., vol. 12, pp. 188-207, 2009.

31) S. Milgram, "The small world problem," Psych. Tod., vol. 1, pp. 61-67, May 1967.

32) S. Easton, and A. Karaivanov, "Understanding optimal criminal networks," Glob. Crim., vol. 10, pp. 41-65, February 2009.