

CRIMINOFÍSICA: UMA APLICAÇÃO AO ESTUDO DA OPERAÇÃO DARKNET

CRIMINOPHYSICS: AN APPLICATION TO THE STUDY OF DARKNET OPERATION

CRIMENOFÍSICA: UNA APLICACIÓN AL ESTUDIO DE OPERACIÓN DARKNET


Submetido em: 17-05-2021.

Aceito em: 24-01-2022.

BRUNO REQUIÃO DA CUNHA

POLÍCIA FEDERAL, PORTO ALEGRE/RS, BRASIL

cunha.brc@pf.gov.br

 <https://orcid.org/0000-0002-9985-6030>

LUIZ WALMOCYR DOS SANTOS JÚNIOR

POLÍCIA FEDERAL, PORTO ALEGRE/RS, BRASIL

walmocyr.lwsj@pf.gov.br

 <http://lattes.cnpq.br/9680097415418363>

JEAN FERNANDO PASSOLD

POLÍCIA FEDERAL, CAXIAS DO SUL/RS, BRASIL

passold.jfp@pf.gov.br

 <http://lattes.cnpq.br/3146047771318653>

RESUMO

Neste artigo, reestudamos, com uma linguagem voltada para a comunidade de Ciências Policiais, a rede de usuários de um fórum de pornografia infantil no navegador *Tor* investigada durante a Operação Darknet da Polícia Federal do Brasil. Essa estrutura criminosa tem características criminofísicas únicas, como uma pequena fração de usuários responsável pelo compartilhamento de mídia ilícita e uma arquitetura de relacionamento muito resistente à intervenção policial. A rede difere das organizações criminosas típicas, aproximando-se, em algum grau, da dinâmica observada em células terroristas.

Ela também apresenta uma topologia análoga à de algumas conhecidas estruturas virais. De outra monta, medidas de correlação como *rich-club* e assortatividade indicam que existe uma cooperação entre pequenos e médios criminosos, enquanto os indivíduos mais proeminentes na rede obtêm apoio do grande número de usuários que apenas visualizam o material ilícito. Por termo, intervenções baseadas em Alvos Topológicos de Alto Retorno indicam que o trabalho policial poderia ter sido 1,6 vezes mais eficiente. Embora a intervenção policial tenha sido, estruturalmente falando, semelhante a ataques aleatórios, ela alcançou alta eficiência ao focar a rede de visualização, já que apenas 10 usuários contribuíram com mais de 1/3 do total de visualizações de postagens e, destes, 8 foram presos pela polícia.

PALAVRAS-CHAVE: criminofísica; ciência de redes; dark web; crimes cibernéticos.

ABSTRACT

In this paper, we re-studied, with a language aimed at the Police Science community, the network of users of a child pornography forum on the Tor browser investigated during the Operation Darknet by the Brazilian Federal Police. This criminal structure has unique criminophysical characteristics such as a small fraction of users responsible for sharing illicit media, and a relationship architecture very resilient to police intervention. The network differs from typical criminal organizations, approaching to some degree the dynamics observed in terrorist cells. It also shows a topology analogous to the structure of many known biological viruses. Correlation measures such as rich-club and assortativity indicate that there is a cooperation between small and medium-sized criminals, while the most prominent individuals in the network get support from the large number of users who only view the illicit material. Interventions based on High Topological Payoff Targets indicate that police work could have been 1.6 times more efficient. While structurally wise police intervention was similar to random attacks, it achieved high efficiency by focusing on the viewing network, as only 10 users contributed to more than 1/3 of the total post views and, of these, 8 were arrested by the police.

KEYWORDS: Criminophysics, Network Science, Dark Web, Cybercrimes.

RESUMEN

En este trabajo, volvimos a estudiar, con un lenguaje dirigido a la comunidad de Ciencia Policial, la red de usuarios de un foro de pornografía infantil en el navegador Tor investigado durante la Operación Darknet por la Policía Federal de Brasil. Esta estructura criminal tiene características criminofísicas únicas, como una pequeña fracción de usuarios responsables de compartir medios ilícitos y una arquitectura de relaciones muy

resistente a la intervención policial. La red se diferencia de las organizaciones criminales típicas, acercándose en cierto grado a la dinámica observada en las células terroristas. También muestra una topología similar a la estructura de muchos virus biológicos. Medidas de correlación como rich-club y asortatividad indican que existe una cooperación entre pequeños y medianos delincuentes, mientras que los individuos más destacados de la red obtienen el apoyo de la gran cantidad de usuarios que solo ven el material ilícito. Las intervenciones basadas en Objetivos de Alta Rentabilidad Topológica indican que el trabajo policial podría haber sido 1,6 veces más eficiente. Si bien la intervención policial estructuralmente inteligente fue similar a los ataques aleatorios, logró una alta eficiencia al centrarse en la red de visualización, ya que solo 10 usuarios contribuyeron a más de 1/3 del total de vistas de publicaciones y, de estos, 8 fueron arrestados por la policía.

PALABRAS CLAVE: Crimenofísica, Ciencia de la red, Web oscura, Cibercriminosos.

1. INTRODUÇÃO

Entre 2014 e 2016, a Polícia Federal deflagrou duas fases da Operação Darknet, que tinha como escopo a investigação criminal de indivíduos envolvidos em um fórum de pornografia infantil em uma plataforma do tipo *dark web* conhecida como rede Tor. Como subproduto da atividade policial, foram identificados 182 criminosos de um total de quase 10 mil usuários, 6 crianças foram resgatadas de predadores sexuais e diversos mandados de busca e apreensão e prisão foram cumpridos (POLÍCIA FEDERAL, 2014, 2016). Após esta fase, o fórum foi desativado por ordem judicial e os dados foram colhidos para análise futura.

De acordo com o Centro Nacional para Crianças Desaparecidas e Exploradas dos Estados Unidos da América e com a Associação de Sites que Advogam a Proteção das Crianças, a exploração de pornografia infantil é um dos negócios online que cresce mais rápido, com um lucro anual estimado em quase 3 bilhões de dólares americanos (ASACP, 2021; NCMEC, 2021). Este tipo de material ilícito geralmente é compartilhado entre ofensores sexuais que o distribuem online, causando danos psicológicos (além é óbvio dos físicos) nas vítimas que duram por toda a vida. Todavia, apesar da gravidade dos delitos envolvendo o compartilhamento de pornografia infantil, muito pouco se sabe sobre as estruturas de rede desses grupos, e menos ainda se sabe sobre a efetividade das intervenções policiais nessa classe de

crime, muito devido à falta de dados e análises confiáveis (CUNHA *et al.*, 2020). Tem-se, pois, dois importantes vazios na literatura que podem ser abordados do ponto de vista das ciências policiais e da criminofísica.

Em especial, a utilização das ciências naturais, entre elas a ciência de redes (MORSELLI, 2009; PAPACHRISTOS, 2011) para compreender como os fenômenos criminais vem ganhando ímpeto com a chamada criminofísica, proposta na obra seminal de mesmo nome (CUNHA, 2021). Nesse ponto de vista, o criminoso passa a ser visto como parte de um dipolo gerador de um “campo” criminal, em analogia, por exemplo, à Teoria Eletromagnética. Em especial, as interações não-lineares entre os elementos constitutivos destes dipolos que faz emergir comportamentos que podem ser explorados por ferramentas já bastante estabelecidas no campo das redes e da física de sistemas complexos. Por exemplo, trabalhos recentes demonstram a importância dos laços fracos na identificação de alvos de alto retorno topológicos em facções criminais (CUNHA, 2018, 2021), bem como verificam que a remoção de apenas 2% desses indivíduos pode causar um verdadeiro “apagão” na rede de crimes federais brasileira (CUNHA; GONÇALVES, 2018). Além disso, já se mostrou que dinâmicas de confinamento implicam em estruturas modulares, o que leva redes criminais a apresentarem fragilidades estruturais que podem ser exploradas pelos órgãos repressivos (SCHNEIDER *et al.*, 2019). A aplicação da criminofísica às redes de pornografia infantil na *dark web* é extremamente recente, mas ela tem o poder de revelar padrões até então desconhecidos.

Nesse sentido, repaginamos aqui artigo anterior dos autores levado ao público anglófono da comunidade de física social (CUNHA, B.R. *et al.*, 2020), agora com o viés das ciências policiais, orientado-o, portanto, ao público nacional. Lançamos mão, então, de ferramentas criminofísicas para entender a dinâmica de relacionamentos entre os criminosos que foram investigados durante a Operação Darknet, mostrando as similaridades e as diferenças entre este grupo e outras redes criminais, explorando suas possíveis fraquezas que poderão ser utilizadas pelos órgãos policiais em futuras investigações similares.

Os dados apresentados neste artigo encontram-se disponíveis,

de forma anonimizada e criptografada, na publicação original dos autores, na base de dados da coleção de física social do periódico *Scientific Reports* da revista *Nature* (CUNHA *et al.*, 2020).

2. A REDE CRIMINAL MEDIADA PELA VISUALIZAÇÃO DE POSTAGENS

Os dados do fórum de pedofilia investigado pela PF foram anonimizados e criptografados. Somente a estrutura de rede foi preservada para este estudo, evitando-se qualquer vinculação dos dados com as pessoas investigadas. Todo o comportamento observado foi emergente, já que o monitoramento era passivo.

Quando um usuário participava do fórum, esta pessoa podia interagir de diversas formas, sendo a mais importante para o presente estudo, a interação por visualização de tópicos, o que demonstrava o interesse de um usuário em outro. Nesse contexto, foi construída uma rede agregada dos dados colhidos durante todo o período de observação, já que não houve acesso a informações temporais ou geoespaciais.

Assim, a rede foi construída da seguinte maneira:

- se um usuário i visualizasse uma postagem do usuário j , uma aresta $i \rightarrow j$ era criada. Se esse mesmo criminoso i interagisse múltiplas vezes com um, ou vários tópicos, do usuário j , então essa aresta continha um peso correspondente à soma dessas atividades.
- Como nessa rede a direção da aresta é importante, em uma aresta do tipo $i \rightarrow j$, o vértice i possuía um grau de saída equivalente ao grau de entrada de j , significando dizer que graus de entrada implicam usuários que recebem visualização de suas postagens e grau de saída que se trata de indivíduos que estão visualizando posts.

Esta rede consiste, então, de um grafo conectado com 10.407 vértices e 842.247 arestas. Assim, a razão variância para média é de 1.369,12, que significa que a distribuição de conexões é super dispersa. Isto pode ser melhor visto quando se verifica que essa mesma razão para as conexões de entrada é de 2.392,34; enquanto que para as conexões

de saída é de apenas 109,26. De fato, apenas 7.4% dos vértices possuem grau de entrada diferente de zero, enquanto que quase a totalidade de usuários apresentam grau de saída maior que zero. A interpretação desses dados é que apenas 769 daqueles indivíduos são, na verdade, os responsáveis pelas postagens da mídia pedofílica, enquanto que 82,6% são usuários que apenas visualizam a pornografia infantil. Como resultado, cada um dos produtores recebia em média 8.208,4 visualizações/postagem, enquanto que para cada produtor 1.095,2 usuários diferentes interagem com seus *posts*, de tal forma que a maioria dos usuários visualizavam a postagem de uma pequena fração de indivíduos.

3. ASPECTOS CRIMINOFÍSICOS

Em redes dirigidas (nas quais a direção da conexão é levada em conta), uma componente fracamente conectada é um subconjunto no qual dois vértices quaisquer estão conectados independentemente da direção de conexão (ESTRADA; KNIGHT, 2015).

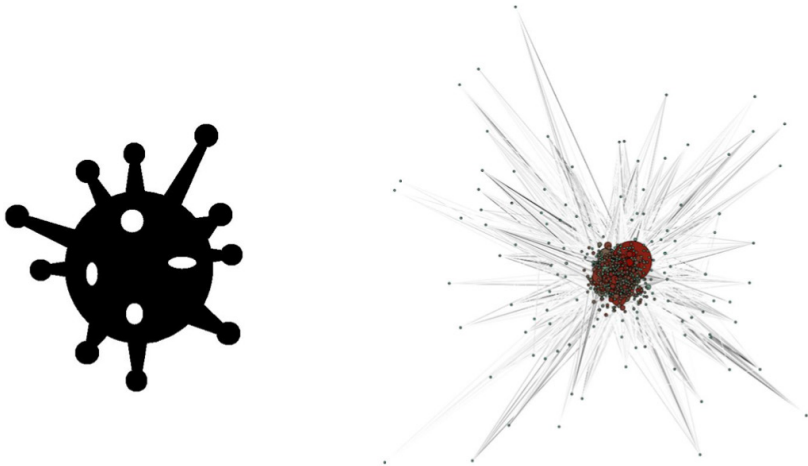
Por outro lado, uma componente fortemente conectada é aquela na qual todos os caminhos relacionais formam um subconjunto conexo seguindo o caminho de conexão. Assim, a rede da Operação Darknet apresenta apenas uma componente fortemente conectada que contém 766 criminosos, enquanto que todos os outros indivíduos são conectados por “espinhos” que se identificam com os usuários que apenas visualizam o material, sem postar nenhum conteúdo ilícito relevante. Por conseguinte, esse núcleo fortemente conexo de 766 delinquentes é quem mantém a rede criminal funcionando organicamente, enquanto que os “espinhos” não possuem um papel estrutural relevante. Analogamente, esta estrutura é surpreendentemente semelhante à de muitos vírus como, por exemplo, o responsável pela atual pandemia de COVID-19, no qual os “espinhos” se assemelham às proteínas *spikes* da SARS-CoV-2 (CUNHA, 2021).

A densidade topológica de uma rede dirigida é definida como o número relativo de arestas em comparação com o número possível de conexões. A densidade de uma rede criminosa geralmente está relacionada ao “brilho” do sistema, no sentido de que um grande número de conexões entre os criminosos significa que se um dos atores fosse preso

seria possível, a princípio, extrair dele informações críticas sobre a estrutura da rede local e de outros participantes (DUIJN; KASHIRIN; SLOOT, 2014). Por outro lado, uma rede mais sombria significa que a transferência direta de informações dentro da rede fica mais lenta devido à diminuição do número de caminhos relacionais possíveis. Portanto, a densidade da rede nos informa sobre a relação entre segurança e comunicação eficaz. Nesse sentido, redes clandestinas que operam ocultas no tecido social, como a de pedófila, têm níveis de densidade muito baixos. Embora a rede completa também tenha uma densidade baixa $D = 0,008$, o componente forte é altamente denso ($D = 0,192$) em comparação com outras redes criminosas conhecidas (CUNHA; GONÇALVES, 2018). Isso pode ocorrer devido ao fato de que os usuários em fóruns do navegador *Tor* tendem a se sentir seguros atrás do sigilo da plataforma e do avatar que usam.

Outra característica marcante das redes reais é que elas tendem a mostrar uma estrutura granular na qual grupos (também chamados de comunidades ou módulos) densamente interconectados estão apenas esparsamente ligados ao resto da rede (DUIJN; KASHIRIN; SLOOT, 2002). Esse comportamento é muito aplicado a redes criminais: enquanto a estrutura de comunidade fortemente conectada facilita a disseminação de informações, a esparsa conexão entre comunidades facilita o sigilo das operações (CUNHA; GONÇALVES, 2017,2018) - uma estrutura típica de compartimentação. A existência de estruturas de comunidade é medida pela modularidade da rede, que é a diferença entre a fração das arestas dentro dos módulos e a fração esperada se a rede fosse aleatória (GIRVAN; NEWMAN, 2002), com valores de Q próximos a 1, indicando estruturas altamente modulares. Apresentando uma modularidade de $Q \approx 0,16$, a rede aqui estudada não possui comunidades bem definidas, diferenciando-a de outras redes criminais.

Figura 1 - À esquerda uma representação esquemática de um vírus biológico e à direita a visualização da rede da operação Darknet da Polícia Federal.



Fonte: Extraída do livro “Criminofísica: a ciência das interações criminais” (CUNHA, 2021).

Geralmente, indivíduos com destaque em determinada rede tendem a se conectar entre si com maior frequência que simplesmente ao acaso, criando um verdadeiro “clube exclusivo” que busca melhor controlar os recursos da rede. Esse fenômeno é conhecido em ciência de redes como “*rich-club effect*”, ou efeito de clube de ricos em tradução livre (ALSTOTT *et al.*, 2014). No *rationale* da criminofísica, a presença desse efeito indica a existência de “hubs” muito conectados entre si, o que pode dificultar futuras intervenções policiais. Matematicamente, o fenômeno é calculado pela proporção de vértices com um número maior de conexões se comparado ao mesmo nó em uma rede com as conexões randomizadas, ou seja:

$$\varphi(k) = E_{\geq k} / N_{\geq k} (N_{\geq k} - 1),$$

onde $N_{\geq k}$ é o número de vértices com grau maior ou igual a k e $E_{\geq k}$ é o número de arestas entre esses nós. Para se obter resultados estatisticamente significantes, este valor deve ser ainda normalizado em relação a um grafo com distribuição de grau aleatória, gerando-se *ensembles* com randomização tanto de arestas quanto de pesos.

A presença do efeito “rich-club” geralmente está associada à cooperação entre indivíduos de determinada “classe” para concentrar as atividades, assim como, a *contrario sensu*, a ausência do fenômeno indica competição entre os membros da rede por acesso aos recursos do sistema (OPSAHL *et al.*, 2008), por postagens *in casu*. O comportamento da rede da Operação Darknet é, neste sentido, curioso e pode ser separado em dois ramos:

1. entre os criminosos com pouca ou média atividade, há intensa cooperação para concentrar a atividade do fórum, o que aumenta conforme cresce o grau de visualização de postagens, gerando um clube de exclusividade de “classe média” com pico em aproximadamente 350 visualizações;
2. já para o terço mais proeminente da rede, essa cooperação desaparece e, conforme os indivíduos se destacam, eles deixam de cooperar e passam a ter comportamentos autônomos, mais próximos do randômico. Isso acontece porque os milhares de usuários que apenas consomem o material ilícito, sem realizar postagens, acabam visualizando diretamente apenas as postagens deste grupo.

Os “rich-clubs” são, na verdade, uma definição estrita de uma medida mais genérica de correlações chamada de assortatividade ou homofilia: enquanto esta mede a conectividade de vértices similares, aquela se presta somente à conectividade de vértices com grau maior ou igual a um determinado limiar. Por exemplo, uma rede consistindo apenas de *hubs* e *spikes*, no qual os *hubs* são muito conectados entre si, é tipicamente desassortativa (*spikes* ligados aos *hubs*), mas com a presença de um clube de exclusividade (*hubs* conectados entre si) - ver Figura 1. Esta é, precisamente, a topologia típica de um vírus (como é o caso das proteínas *spikes* no SARS-CoV-2), que se repete na rede de usuários da *Darknet*, que apresenta uma desassortatividade de aproximadamente -0,21. Essa analogia à estrutura viral não se limita por aí. Em redes de negócios, por exemplo, *players* altamente populares tendem a se conectar com outros também proeminentes para manter sua reputação e status. Todavia, algumas redes virtuais são conhecidas por serem desassortativas. É, novamente, o caso em estudo aqui, no qual os usuários não estão interessados em manter o fórum por status social ou reputação, de modo que não há competição estatística relevante entre

os usuários por postagens. Os resultados da análise mostram que os criminosos estão mais interessados em saciar a sua lascívia por pornografia infantil, independentemente de qual a fonte daquele material. Destarte, vemos um pequeno número de usuários visualizando conteúdo e tendo seu conteúdo visualizado de forma desproporcional, em comparação com o resto.

Nesse aspecto arquitetônico, pode-se dizer que redes de pornografia infantil se aproximam topologicamente de redes de terrorismo, que também apresentam algum nível de desassortividade, diferentemente de redes de crime organizado, por exemplo.

4. EFICIÊNCIA TOPOLÓGICA DA AÇÃO POLICIAL

Durante a Operação Darknet, os investigadores definiram uma pirâmide qualitativa de prioridades de acordo com a gravidade das condutas individuais: os usuários mais sensíveis foram aqueles que aparentemente cometiam abusos na vida real, seguidos por grandes compartilhadores de conteúdo e, em seguida, por usuários que apenas realizaram o download de conteúdo pornográfico infantil. Posteriormente, os usuários começaram a ter sua identidade revelada a partir de técnicas de remoção de anonimato em comunicação por meio da rede *Tor*. Em seguida, iniciou-se a investigação criminal tradicional e os investigadores buscaram mais evidências do envolvimento de cada indivíduo, com suas próprias idiossincrasias e desafios investigativos. Além disso, algumas situações especiais obrigaram os investigadores a contornar a pirâmide de gravidade algumas vezes. Por exemplo, embora o objetivo da polícia fosse alcançar o maior número de criminosos, o processo técnico de identificação de indivíduos reais a partir do navegador *Tor* era demorado e dependente de muitas questões práticas, como o nível de experiência em camuflagem de cada usuário, ao passo que, devido a requisitos legais, a investigação teve um prazo limitado. O resultado das duas fases da investigação foi 176 criminosos identificados na vida real e presos por compartilhar ou armazenar mídia contendo pornografia infantil, e 6 presos por estupro de vulnerável - desse total, 170 eram compartilhadores (22% do componente forte) e 12 eram *spikes*.

Os recursos das forças policiais são limitados por diversos motivos, das muitas limitações legais às de caráter operacional. Portanto, é crucial saber a quantidade mínima de alvos que devem ser priorizados para se romper a estrutura de rede da macrocriminalidade. Este problema é conhecido na criminofísica como intervenção mínima para ruptura de rede (CUNHA; GONZÁLEZ-AVELLA; GONÇALVES, 2015) (CUNHA, 2017) (ABREU; ASSLANI *et al*, 2020) (GONÇALVES; CUNHA, 2021). Sob a óptica da criminofísica, uma rede criminal é um grafo composto por criminosos (vértices) conectados entre si de acordo com seu relacionamento (arestas), que podem ser multifatoriais como chamadas telefônicas, agressão, informação de inteligência, etc.

Nesse contexto, a heterogeneidade de uma rede é uma característica fundamental no estudo de sua robustez (BARABÁSI, 2016). Por exemplo, redes aleatórias se despedaçam após a falha de um pequeno número crítico de alvos. Por outro lado, redes com distribuições heterogêneas (de graus de cauda pesada em um linguajar mais matemático) são geralmente muito frágeis a ataques direcionados a alvos-chave, quando um “apagão” completo da rede é novamente obtido, num verdadeiro efeito dominó, após a remoção de uma pequena fração de vértices - conhecidos como Alvos Topológicos de Alto Retorno (ATAR) no contexto de redes criminais (CUNHA, 2021). A maioria das redes criminais conhecidas têm distribuições de graus de cauda pesada.

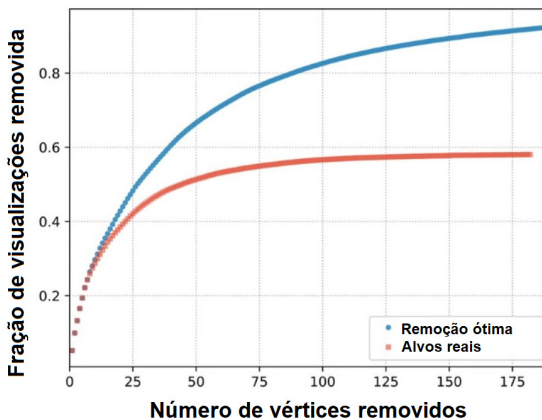
De um modo geral, as intervenções das forças policiais objetivam identificar e prender criminosos. Tal procedimento resulta em uma interpretação topológica simples: quando um criminoso é preso, uma fração dos seus relacionamentos é cortada. Essa remoção é sabidamente menos efetiva se comparada com estratégias de remoção total de relacionamento (confinamento em solitária) ou a completa remoção de criminosos através de ressocialização ou morte. Todavia, em se tratando de redes online, os alvos são apenas avatares de pessoas reais e sua simples prisão resulta em sua completa remoção da rede, ou seja, uma típica estratégia de neutralização.

Apesar de, nessa rede, um pequeno número de usuários compartilhar a maior parte do conteúdo, o núcleo duro é muito denso. Neste caso, essa rede é mais heterogênea que as redes de crime organizado, tendo uma distribuição matemática compatível com exponen-

ciais e Gaussianas. Isso indica também que o núcleo é muito resiliente a intervenções. Na verdade, seria necessária a remoção aleatória de todos os usuários ou a remoção de quase 60% dos indivíduos, de acordo com a melhor estratégia ATAR, ou 1,6 vezes mais eficiente que o resultado da pirâmide de gravidade qualitativa proposta pelos investigadores.

Embora a topologia da rede seja muito robusta, a maioria das postagens é compartilhada por uma pequena fração dos usuários, então, podemos ter uma abordagem mista para analisar essa rede. Uma baseada na arquitetura dos relacionamentos criminais e outra com foco naquilo que alimenta a rede em si: as postagens compartilhadas. Na Figura 2, mostramos o resultado da remoção dos nós em ordem de grau ponderado (círculos azuis). A remoção dos 100 alvos principais reduz as visualizações de postagem em 82,6%. Os quadrados vermelhos representam a remoção dos usuários presos. Inicialmente, houve muita eficiência com 8 dos 10 principais participantes presos, tendo esta primeira dezena contribuído com mais de um terço de todo o conteúdo compartilhado. Com 20 prisões conseguiu-se 38,5% de acerto ante uma redução teórica máxima de 42,8% de postagens. Os alvos subsequentes foram selecionados de forma menos otimizada, de modo que o total de prisões reduziu as postagens em 58,1% de possíveis 91,9%, de modo que metade das visualizações de postagem em toda a rede pode ser atribuída a apenas 28 usuários que postaram conteúdo.

Figura 2 - A fração de visualizações removidas em função do número de vértices também retirados conforme os efeitos reais da operação (quadrados vermelhos) e a remoção ótima teórica (círculos azuis).



Fonte: Extraída do artigo original dos autores em CUNHA *et al.*, 2020.

5. CONCLUSÃO

Neste trabalho, rerepresentamos uma rede criminal intermediada por visualizações de tópicos postados em um fórum de pornografia infantil na dark web, trabalho já publicado pelos autores (DA CUNHA *et al.*, 2020) no contexto da física social. Trouxemos aqui uma abordagem voltada às ciências policiais e ao público lusófono, apresentando os aspectos criminofísicos deste sistema, suas características e fragilidades que podem ser abordadas em intervenções policiais.

A rede original consiste em 10.407 usuários, dos quais apenas 766 pertencem a um núcleo duro que é, de fato, responsável pelas postagens contendo mídia ilícita. A pesquisa constatou 9.638 criminosos que não postaram qualquer conteúdo online, mas mantiveram visualizações constantes do material pedofílico. Esses indivíduos possivelmente seguiam o fórum por curiosidade e inclinação pedofílica, mas a atividade se revelava como uma porta de entrada para as atividades criminais mais sérias que ocorriam no núcleo da rede. Os criminosos pertencentes ao núcleo duro da rede compunham um subgrupo extremamente ativo tanto na visualização quanto no compartilhamento de conteúdo, sendo os responsáveis por estruturar toda a empreitada criminosa.

Este aglomerado central de criminosos apresenta algumas diferenças marcantes com relação a redes criminais típicas. Por exemplo, o crime organizado apresenta uma tendência criminofísica a se estruturar em topologias modulares, algo que não é presente na rede de pedofilia aqui trabalhada. Essa característica possui duas interpretações importantes. A primeira é que os usuários do fórum não apresentam estatisticamente interesse particular em apenas alguns tópicos, eles costumam interagir com uma ampla gama de *threads*. A segunda interpretação está relacionada ao fato de que o fenômeno de modularidade está geralmente associado a cenários competitivos como crime organizado, mercados financeiros e sistemas do tipo predador-presa. Contudo, o núcleo duro da rede de pedofilia consiste em indivíduos mais interessados em cooperar para saciar suas necessidades de consumo patológicas. Essa arquitetura singular se assemelha muito à de alguns vírus, como, por exemplo, o SARS-CoV-2 (não passando, contudo, de relação puramente análoga, sem maiores semelhanças funcionais).

Outra característica importante está associada ao brilho da rede. Estruturas clandestinas geralmente apresentam baixa densidade de arestas como forma de ocultar suas atividades da fiscalização policial. Entretanto, esse não é o caso do núcleo duro desta rede, já que usuários da dark web, mais precisamente do *Tor* browser, costumam se sentir seguros escondidos atrás de avatares e de vários graus de anonimidade. Isso faz com que usuários desse tipo de plataforma tendam a agir de maneira mais livre, sem se preocupar tanto com o balanço entre eficiência e clandestinidade típicos de organizações criminosas. Outrossim, a anonimidade de um avatar fantasioso bloqueia alguns mecanismos psicológicos como a busca indireta por prestígio através de aparências, como mostrado pelo índice de desassortividade da rede de pedofilia da Operação Darknet.

Apesar da desassortatividade da rede, há um um clube de exclusividade médio que desaparece para vértices muito conectados. Esse comportamento mostra que a rede é robusta a intervenções policiais. De fato, o núcleo duro só pode ser desmantelado após a remoção de aproximadamente 60% dos seus componentes, o que se mostra em alto contraste com redes criminais típicas que costumam ser muito mais frágeis. Isso ocorre devido à topologia característica dessa rede.

De outra monta, a polícia foi bastante eficiente em identificar aqueles criminosos que pertenciam ao núcleo duro da rede - 170 dos 182 usuários foram alvos de medidas restritivas. Entretanto, as intervenções policiais foram tão eficientes quanto remoções aleatórias de indivíduos e mesmo o melhor ataque do tipo ATAR melhoraria essa eficiência em apenas 1.6 vezes. Destarte, os resultados apontam que a melhor abordagem seria manter operações de monitoramento contínuas até que um número suficientemente grande de criminosos pertencentes ao núcleo duro fosse identificado. Outra possibilidade seria monitorar diversos fóruns à procura de usuários reincidentes que não poderiam ser mantidos alvos em outras investigações.

Por outro lado, ao focarmos nos usuários que atraem a maioria das visualizações, a quantidade de interações deve diminuir de maneira muito mais eficiente do que a quebra direta de toda a estrutura. Assim, apesar da estrutura da rede ser muito robusta, ainda podemos romper significativamente a quantidade de visualizações. Isso porque apenas

16 usuários contribuíram para quase a metade das visualizações de postagens. Nesse sentido, 10 desses criminosos foram presos pela polícia, o que significa uma acurácia de 80% na identificação daqueles usuários que atraíam a maioria das visualizações. Além disso, os investigadores conseguiram remover aproximadamente 60% dos post views com a prisão de 182 usuários, uma taxa bastante eficiente se considerarmos o máximo teórico de 90%. Destarte, ao se afastar criminosos que concentravam a quantidade de visualizações, essa atividade se reduziria significativamente, impedindo a atividade principal do fórum que seria inativado por “inanição”, resultando em fragmentação indireta.

Tais resultados podem ajudar investigadores a planejar intervenções policiais futuras mais eficientes em cenários similares ao aqui estudado, ou seja, redes de saciedade como as de pedofilia, as de ódio e as terroristas.

BIOGRAFIA DOS AUTORES:

BRUNO REQUIÃO DA CUNHA

PÓS-DOCTOR EM MATEMÁTICA APLICADA (UNIVERSITY OF LIMERICK, IRLANDA);

DOUTOR EM FÍSICA TEÓRICA (UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL);

AGENTE DE POLÍCIA FEDERAL.

LUIZ WALMOCYR DOS SANTOS JÚNIOR

ENGENHEIRO ELETRICISTA (UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL);

AGENTE DE POLÍCIA FEDERAL.

JEAN FERNANDO PASSOLD

FARMACÊUTICO (UNIVERSIDADE FEDERAL DE SANTA CATARINA);

BIOQUÍMICO (UNIVERSIDADE FEDERAL DE SANTA CATARINA);

PAPILOSCOPISTA POLICIAL FEDERAL.

REFERÊNCIAS

- ALSTOTT, J. *et al.* A unifying framework for measuring weighted rich clubs. *Scientific reports*, v. 4, n. 1, p. 1-6, 2014. Disponível em: <<https://doi.org/10.1038/srep07258>>. Acesso em: 12 mai. 2021.
- ASACP. [Statistics], 2021. Disponível em: <<https://www.asacp.org/index.html?content=statistics>>. Acesso em 12 mai. 2021.
- ASLLANI, Malbor *et al.* Dynamics impose limits to detectability of network structure. *New Journal of Physics*, v. 22, n. 6, artigo 063037, 2020. Disponível em: <<https://doi.org/10.1088/1367-2630/ab8ef9>>. Acesso em: 12 mai. 2021.
- BARABÁSI, A.L. *Network Science*. Cambridge: Cambridge University Press, 2016.
- CUNHA, B.R. *Estudo sobre a topologia das redes criminais*. 2017. 84 f. Tese (Doutorado em Física Teórica) - Instituto de Física, Universidade Federal do Rio Grande do Sul, Porto Alegre, Tese de Doutorado, 2017. Disponível em: <<https://www.lume.ufrgs.br/handle/10183/169125>> . Acesso em: 12 mai. 2021.
- CUNHA, B.R. Argumento topológico para a priorização de alvos-chave em organizações criminosas. In: BALDAN, E.L.; FERNANDES, A.P.P. *Ciências policiais e segurança pública*. 1 ed. Goiânia: Ilumina, 2018. p. 234-236.
- CUNHA, B.R. Affronter les factions criminelles et le crime organisé au Brésil: le recours à la science des réseaux. In: DOLO, N.; RACOUCHOT, B. *Brésil; corruption, trafic, violence, criminalité; vers la fin du cauchemar?* Collection Sécurité Globale. Paris: MA Editions - ESKA, 2018. p. 234-236.
- CUNHA, B.R. *Criminofísica: a ciência das interações criminais*. Editora Buqui, 2021.
- CUNHA, B.R. Neutralização Seletiva de Alvos Topológicos de Alto Retorno em Facções Criminosas. *Revista Brasileira de Ciências Policiais*, v. 12, n. 4, p. 53-73, 2021. Disponível em: <<http://dx.doi.org/10.31412%2Frbcv12i4.616>>. Acesso em: 12 mai. 2021.
- CUNHA, B.R. *et al.* Assessing police topological efficiency in a major sting operation on the dark web. *Scientific reports*, v. 10, n. 1, p.

1-10, 2020. Disponível em: <<https://doi.org/10.1038/s41598-019-56704-4>>. Acesso em: 12 mai. 2021.

CUNHA, B.R.; GONÇALVES, S. Performance of attack strategies on modular networks. *Journal of Complex Networks*, Oxford, v. 5, n. 6, p. 913-923, 2017. Disponível em: <<https://doi.org/10.1093/comnet/cnx015>>. Acesso em: 12 mai. 2021.

CUNHA, B.R.; GONÇALVES, S. Topology, robustness, and structural controllability of the Brazilian Federal Police criminal intelligence network. *Applied Network Science*, v. 3, n. 1, p. 36, 2018. Disponível em: <<https://doi.org/10.1007/s41109-018-0092-1>>. Acesso em: 12 mai. 2021.

CUNHA, B.R.; GONZÁLEZ-AVELLA, J.C.; GONÇALVES, S. Fast fragmentation of networks using module-based attacks. *PLoS one*, São Francisco, v. 10, n. 11, p. e0142824, 2015. Disponível em: <<https://doi.org/10.1371/journal.pone.0142824>>. Acesso em: 12 mai. 2021.

ABREU, C.; GONÇALVES, S.; DA CUNHA, B.R. Empirical determination of the optimal attack for fragmentation of modular networks. *Physica A: Statistical Mechanics and its Applications*, v. 563, p. 125486, 2021. Disponível em: <<https://doi.org/10.1016/j.physa.2020.125486>>. Acesso em: 12 mai. 2021.

DUIJN, P.A.C.; KASHIRIN, V.; SLOOT, P.M.A. The relative ineffectiveness of criminal network disruption. *Scientific Reports*, v. 4, p. 4238, 2014. Disponível em: <<https://doi.org/10.1038/srep04238>>. Acesso em: 12 mai. 2021.

ESTRADA, E.; KNIGHT, P.A. *A first course in network theory*. Oxford: Oxford University Press, 2015.

GIRVAN, M.; NEWMAN, M.E.J. Community structure in social and biological networks. *Proceedings of the National Academy of Sciences*, Washington, v. 99, n. 12, p. 7821-7826, 2002. Disponível em: <<https://doi.org/10.1073/pnas.122653799>>. Acesso em: 12 mai. 2021.

MORSELLI, C. *Inside criminal networks*. Nova Iorque: Springer, 2009.

NCMEC. [Case resources], 2021. Disponível em: <<https://www>.

missingkids.org/ourwork/caseresources>. Acesso em: 12 mai. 2021.

OPSAHL, T.; COLIZZA, V.; PANZARASA, P.; RAMASCO, J.J. Prominence and Control: The Weighted Rich-Club Effect. *Phys. Rev. Lett.* 101, 168702. Disponível em: <<https://doi.org/10.1103/PhysRevLett.101.168702>>. Acesso em: 12 mai. 2021.

PAPACHRISTOS, A.V. The coming of a networked criminology? In: MACDONALD, J. *Measuring Crime and Criminality: Advances in Criminological Theory*. Nova Jersey: Transaction Publishers, 2011. p. 101-140.

POLÍCIA FEDERAL. [*Operação Darknet – Balanço*]. Brasília, 2014. Disponível em: <<http://www.pf.gov.br/agencia/noticias/2014/10/operacao-darknet-balanco>>. Acesso em: 12 mai. 2021.

POLÍCIA FEDERAL. [*PF divulga balanço da Operação Darknet II*]. Brasília, 2016. Disponível em: <<http://www.pf.gov.br/agencia/noticias/2016/11/pf-divulga-balanco-da-operacao-darknet-ii>>. Acesso em: 12 mai. 2021.

SCHNEIDER, E. *et al.* Dynamic Modular Networks Model Mediated by Confinement. *Applied Network Science*, v. 4, n. 1, 2019. Disponível em: <<https://doi.org/10.1007/s41109-019-0143-2>>. Acesso em: 12 mai. 2021.

INFORMAÇÕES ADICIONAIS E DECLARAÇÕES DOS AUTORES

(*integridade científica*)

Declaração de conflito de interesse: O(s) autor(es) confirma(m) não haver conflitos de interesse na condução desta pesquisa e na redação deste artigo.

Declaração de autoria: Todos e apenas os pesquisadores que atendem os requisitos de autoria deste artigo são listados como autores; todos os coautores são integralmente responsáveis por este trabalho em sua totalidade.

Declaração de originalidade: O(s) autor(es) assegura(m) que o texto aqui publicado não foi previamente divulgado em qualquer outro local e que a futura republicação apenas será feita com expressa referência desta publicação original; também atesta(m) que não há plágio de material de terceiros ou autoplágio.

COMO CITAR (ABNT BRASIL)

REQUIÃO, Bruno da Cunha; SANTOS JUNIOR, Luiz Walmocyr dos; PASSOLD, Jean Fernando. Criminofísica: uma aplicação ao estudo da operação darknet. *Revista Brasileira de Ciências Policiais*, Brasília, vol. 13, n. 8, p. 95-113, mar. 2022.

<https://doi.org.br/10.31412/rbcp.v13i8.932>



ESTA OBRA ESTÁ LICENCIADA COM UMA LICENÇA CREATIVE COMMONS ATRIBUIÇÃO-NÃO COMERCIAL 4.0 INTERNACIONAL.