The social network analysis and hackers' networks

Olga Smirnova, Associate Professor, MPA, Department of Political Science, East Carolina University, smirnovao@ecu.edu

ABSTRACT: The online market for stolen data creates unique networks via comments or other relations between various players. The available information serves as a valuable resource to apply social network (SNA) methods to assess offender networks. These methods focus not only on the players but on the connections between the players, and imply that the transfer of information in the market demonstrates key associations between actors. SNA methods allow for the identification of key players on a network and can be useful for law enforcement to develop targeted takedown strategies of important dark networks. Additionally, it may provide a limited predictive capacity to identify key-players before any arrests have been made.

Online markets on the Open or Dark Web enable the exchange of information as well as goods and services. While the trade of physical products requires some face to face interactions, the sale of cybercrime services may happen completely online. The visible informational exchanges between actors allows researchers to build connections between various users and assess hidden networks that may exist. Social network (SNA) methods emphasize connections between players through *relational ties* based on trade and social status.

Certain activities such as finding criminal collaborators or advertisements for goods and services happen more in the online forums and shops. SNA allows for the interdependent nature of market relationships where the quantity of goods sold depends on the feedback vendors receive from buyers. The buyers' reputation allows them access to special market tiers that may not be available to outsiders.

Online markets share characteristics with various forms of illicit operations in the real world, and legitimate market operating online. For instance, forums allow for communication between buyers and sellers including online retailers' reviews. These posts, particularly reviews, create social networks of dark market actors. These relational ties facilitate the flow of information about available goods and prices, credibility of both buyers and sellers, as well as actual trades of digital goods and services.

At the same time, shops which operate as single vendor markets on independent websites allow buyers to contact sellers via convenient forms; these shop connections are usually visible only to the shop owner/operator. As a result, it is more difficult to build the networks between shop participants as they do not typically allow for direct comments to be posted by users.

There are different *relations* that may exist between key players such as comments to each other, private messages, mentions of users, the IP addresses used, the geographic locations of registrations, targeted victims, languages used, and more. All of these pieces of information serve as *relations* to build *relational ties* or links between users.

As an example, many vendors in illicit online markets now utilize Bitcoin as their payment method of choice. The Bitcoin wallets associated with vendors can serve as a key point of attribution which can be observed and used to build relational ties.

Similarly, the diversity of products sold varies from platform to platform. "Open" web platforms contain a wide range of items from all over the world. Dark web vendors often target specific countries or regions, such as US or EU. The products include: stolen data (card numbers and other personal identifiable information useful for identity fraud), drugs, guns, prostitution, hit and murder services.

These connections also allow the researchers to use SNA methods that have been applied to various connections in the real and digital world between individual actors.

Examples of SNA

SNA can be further subdivided into confirmatory and exploratory analyses. Confirmatory analyses such as Decary-Hetu and Dupont (2012) and Leukfeldt et al (2017) use information from actual arrest data regarding key players and networks. Such analyses are only possible after taking down the whole network. These studies have access to the

personal messages and often confirm who are the key players as well as identify other potential key actors (not yet apprehended). However, this type of analysis captures the activities and networks between actors post-arrest, which may not reflect the most current structures.

The exploratory SNA such as in Holt et al (2016), Smirnova and Holt (2017) provide the most current information of networks, as a census of what is going on in the dark markets. While this type of analysis may also identify key players, there is no 'confirmation' of specific roles these actors play in criminal networks as noted in other studies.

Additionally, SNA methods allow to study global and local characteristics of networks. SNA local analysis focuses on the individual position on the networks and its characteristics. For example, one can measure the number of connections or interactions one made on a forum (*degree centrality*). SNA global analyses focus on overall network characteristics. The global SNA takes the collection of all links and derives network-wide measures that may characterize an online forum or community. The basic premise is that information flows through these connections, and the connections themselves form an entity. The transfer of information results in the underlining structure that can be depicted on the networks. Figure 1 shows the depiction of TOR shops network: the *relational ties* here are based on the same IP address used by a shop.

There is a tradeoff between efficiency and resilience on a network. The most efficient network is a hierarchical structure where each component can serve its unique purpose, but the most resilient structure is the distributed network where taking down any individual component will not have any global impacts on the overall network and network can easily rebound. In this regard, the online dark market networks are not very efficient as they have a lot of redundancies, but these redundancies make them more resilient to the outside shocks.

Policy Implications

Due to the robust nature of online dark markets, there is a need to understand how to best affect the communities that support the illicit exchanges in fee-for-service markets. Potential market disruption strategies should differentiate the nature of the advertising space. Forums provide a centralized location that could be taken over. The decentralized nature of shops means one vendor could operate with multiple faces. Slander attacks within forums or reporting shop vendors as rippers to reporting repositories could tackle the main component that flows through a network: reputation and information.

Additionally, education of consumers and development of good business practices may provide some cybercrime prevention strategies.

In all instances, actors can displace to other markets rapidly. Hence, efforts may also be directed toward ancillary providers/resources such as payment providers, bulletproof hosting, or shipping.

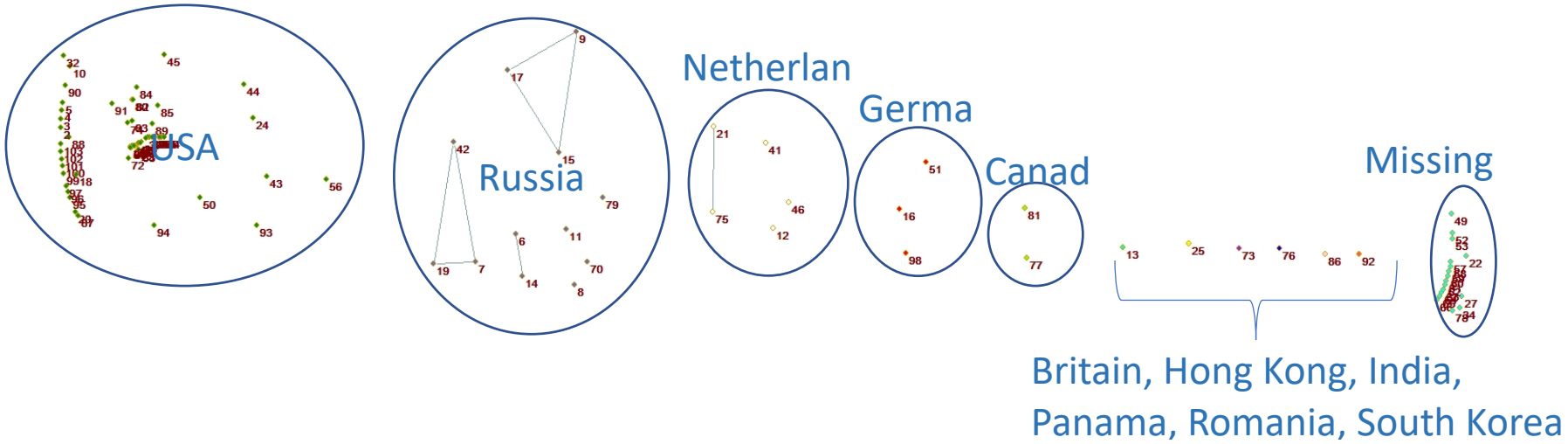

FIGURE 1. The TOR shops networks based on the IP addresses used by the shops. The connected shops share the same IP address. The shops are sorted by various countries they are registered in. Two of the connected subgroups in Russia are registered in Moscow, and one in Saint Petersburg. The connected shops in the Netherlands are registered in Amsterdam.

REFERENCES: This white paper draws on the research conducted for the larger project "Understanding the Economy and Social Organization for the Underground Market for Cybercrime as a Service" funded by Criminal Investigations and Network Analysis (CINA) A DHS Center of Excellence George Mason University (United States Department of Homeland Security). The brief also draws on these articles:

Décary-Hétu, D., & Dupont, B. (2012). The social network of hackers. *Global Crime*, *13*(3), 160-175.

Holt, T. J., Smirnova, O., & Hutchings, A. (2016). Examining signals of trust in criminal markets online. *Journal of Cybersecurity*, *2*(2), 137-145.

Leukfeldt, R., Kleemans, E., & Stol, W. (2017). The use of online crime markets by cybercriminal networks: A view from within. *American Behavioral Scientist*, *61*(11), 1387-1402.

Smirnova, O., & Holt, T. J. (2017). Examining the Geographic Distribution of Victim Nations in Stolen Data Markets. *American Behavioral Scientist*, *61*(11), 1403-1426.