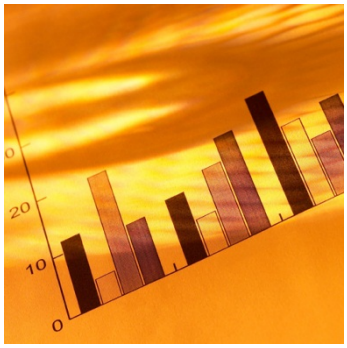
RESEARCH HIGHLIGHTS

Organized Crime



2016 – H004

www.publicsafetycanada.gc.ca

BUILDING A **SAFE** AND **RESILIENT** CANADA

CRIMINAL NETWORK DISRUPTION

Disrupting emerging criminal networks is most effective

Developing effective law enforcement strategies to control and disrupt organized criminal networks is a difficult task. Empirical evidence from social network analyses has illustrated the fluidity and flexibility that many criminal networks possess, making them highly resistant against traditional law enforcement strategies aimed at targeting the leaders or 'kingpins' of the criminal organization. While research has identified flexibility as a crucial feature that protects criminal networks from disruption, little is known about how criminal networks actually adapt and recover from an attack.

This study combines social network analysis and computational modelling to simulate the behaviour of an illicit cannabis cultivation network in the Netherlands. The organized cultivation of cannabis through illegal networks is a problem faced by many countries, and law enforcement attempts at mitigating this problem are often unsuccessful. The aims of the research were to examine the dynamics of criminal network resilience against disruption and also to identify the most effective disruption strategy. The latter aim was achieved by simulating the effects of five different disruption strategies on the criminal network using their model.

The authors distinguish between two common approaches for criminal network disruption. The social capital approach involves identifying the actors in the network with the most social capital, that is, those in influential or powerful positions. While useful, the leadership of criminal networks is often fulfilled by multiple actors, of which some are not always in the most central and easily identifiable positions. In contrast, the human capital approach identifies actors in the criminal network through their individual qualities, attacking the criminal network by targeting the actors that possess the most specialized and valuable sets of skills and knowledge required in the illegal activity. The authors use the term 'value chain' to refer to the chainlike structure existing in the business process of all criminal markets. Each step required to undertake an illegal activity requires different levels of information, goods, and human capital. Thus, roles can be identified and targeted that are valuable to the chain. To counter these strategies, criminal networks develop the capacity to withstand disruption and adapt to changes, if necessary. This is known as criminal network resilience.

The study consisted of two aggregated datasets. The first set consisted of intelligence gathered by a unit working for the Dutch Police from January 2008 to January 2012. This included data about organized

In This Issue

crime gathered from criminal informants and reports from closed organized crime cases. The second set consisted of arrest records in the same region during the same time period. By combining these two sets of data, the authors were able to recover the structure of a criminal network in the Netherlands that was involved in multiple criminal markets.

After constructing a socio-graph of the criminal network, the authors removed all actors not involved in cannabis cultivation. A value chain was then created that described the roles and flow of human capital involved in the cannabis cultivation network. It was found that some roles were common and highly connected (i.e. easily replaceable) within the chain, and others not. The roles of 'Coordinator' and 'Growshop Owner' were singled out as important links that kept the value chain together, and were identified as vulnerable targets for both disruption approaches. The role of the 'Specialist' was also identified as a vulnerable target, which consisted of individuals in highly specialized roles, such as those responsible for manipulating the electrical supply of the grow-op.

Simulations were run on the combined dataset to test common law enforcement disruption strategies and criminal network resilience in order to measure the effects on the network. The disruption strategies tested two types of social capital disruption, two types of human capital disruption, and a random disruption. To model the different ways criminal networks recover from disruption, three algorithms were introduced that simulated different forms of criminal network recovery. It was found that all network disruption strategies were ineffective at disrupting the network. However, in some cases the efficiency of the network actually increased, with disruption strategies creating a more resilient drug network. These results show the flexibility and adaptive structure of the cannabis cultivation network which make it highly resilient to law enforcement disruption strategies.

This study reveals that intervention into a recently established criminal network is more effective than interference with one that is older. The phenomenon where disruption strategies lead to a more resilient criminal network is likely due to the original network operating inefficiently, with no need to evolve or expand. The impact of the disruption strategy forces the network to reorganize itself in a more productive manner, making it more efficient than in its previous state.

The authors note that "in practice this means that disrupting a criminal network involves a long-term consistent intervening effort" (14). While disruption strategies may cause the network to become more efficient in the short term, over time this will gradually increase the visibility of the criminal network, forcing it out "from the dark" (14). As this occurs, the criminal network will become less secure and new opportunities for surveillance and intelligence gathering will open up for law enforcement to identify and target the future replacements for central actors in the network. Eventually, "cracks in the network structure will emerge in the long run" (14), allowing for more specific and deliberate disruption strategies.

Duijn, P.A.C., Kashirin, V. & Sloot, P.M.A. (2014). "The relative ineffectiveness of criminal network disruption." *Scientific Reports*, 4 (4238): 1-15.

APPLYING SOCIAL NETWORK ANALYSIS TO MONEY LAUNDERING DETECTION

SNA can improve the speed and accuracy of money laundering investigations

Social Network Analysis (SNA) is a multidisciplinary approach that can map and measure the relationships between entities in a social network, such as people, groups and organizations. SNA is also a valuable analytical tool for law enforcement. When utilized effectively, SNA can identify sophisticated criminal networks and detect the roles and ties between members.

This study involves applying SNA to money laundering detection. Money laundering is a criminal offence that occurs when the proceeds of crime are disguised to make them appear legal. This allows criminals to freely control their assets derived from crime, and also conceals the identities of the persons involved in illegal practices from the authorities. The authors apply SNA algorithms to a Money Laundering Detection System (MLDS), a module designed to detect money laundering by analyzing money transfers in a banking system.

Using the MLDS module, the authors present a system that constructs social networks from bank statements and the National Court Register (in Polish, KRS). The

KRS is a publically available, computerized database that contains information on registered entities. This includes extensive registers of businesses, associations, other organizations, foundations, public health care institutions and insolvent debtors. A series of questions were developed to aid in the identification of roles in the network, which was necessary for the SNA. This included questions such as, if multiple business entities have the same registered office address, and if this address was located in a country put on the "black list" for offering more advantageous fiscal conditions.

The authors used SNA to perform an analysis on the network, which allowed them to detect its vulnerabilities and identify the particular people in leadership positions. A series of algorithms were implemented to uncover the structure of connections between roles, and whether multiple bank accounts were registered to the same person. Cluster techniques and frequent pattern mining were other statistical approaches used in conjunction with SNA to uncover roles of persons in the network. Clusters are sets of money transfers that are treated as suspected money laundering operations due to fulfilling specific criteria. Clusters that are found can be mined for frequent sets and sequences to identify money laundering and the roles of the entities involved. This particular approach allowed the authors to uncover suspicious activity in the network and groups of offenders.

The authors conclude that SNA can provide a valuable tool for investigations into money laundering. Using available data such as bank statements and registers that contain relevant data, this technique can identify patterns of offenders and their roles in the criminal network. They also stress the importance of other advanced analytic techniques, such as data mining, machine learning, and data clustering as tools that can help law enforcement and policymakers develop strategies to prevent the organized crime of money laundering.

Drezewski, R., Sepielak, J., Filipkowski, W. (2015). "The application of social network analysis algorithms in a system supporting money laundering detection." *Information Sciences* 295, 18-32.

See also:
Drezewski, R., Sepielak, J., Filipkowski, W. (2012). "System supporting money laundering detection." *Digital Investigation, 9(1),* pp. 8–21.

CHALLENGES FACED IN COUNTER CYBERCRIME OPERATIONS

Many technical challenges and legal barriers are encountered during cybercrime operations

The modern fight against cybercrime requires that law enforcement and the judiciary have extensive knowledge of computer technology and keep up to date with cutting-edge developments in network security. Cybercrime is a global phenomenon and is constantly expanding as the knowledge and tools required to commit such acts have become easily accessible for the everyday public. This has generated sophisticated criminals whose expertise and tools often equal or outmatch the capabilities of law enforcement. At the same time, techniques employed to battle cybercrime are bound to criminal procedure that has to be consistently adapted to new circumstances.

This article examines the challenges encountered by law enforcement and Signals Intelligence (SIGNET) agencies in regards to counter cybercrime operations. The author presents a case study of the law enforcement operation against the online black market, "Silk Road." The obstacles that were encountered during this operation are discussed, followed by a section outlining the legal boundaries and instruments used to overcome technical challenges. Finally, a section is presented on Signals Intelligence (SIGINT) agencies and their role in counter cybercrime operations.

The two major safeguards that secured Silk Road's server location and identity of the owner were the use of the Tor network and limiting payment to only one system, Bitcoin. Tor is an extremely effective software that enables anonymous communication by obscuring the Internet Protocol (IP) addresses of its users. Bitcoin is a form of virtual currency in use throughout the world. It is decentralized and anonymous, meaning that no single organization controls it and it can be used without registering personal details. Along with traditional methods of policing, the owner of Silk Road was eventually apprehended through electronic methods of investigation.

Several technical and legal challenges arose from the investigation, notably the problem of unbreakable encryption solutions used by Tor. These hide IP addresses and protect data, preventing law enforcement from gaining access to evidence. It is also currently

mathematically impossible to break certain encryption solutions. At the same time, even if the key is known, there are several encryption programs that can keep incriminating data hidden if the user is forced to decrypt data. Because of these obstacles, law enforcement has to circumvent unbreakable encryption solutions and exploit the negligent behaviour of perpetrators, which was the case in the Silk Road investigation. As of now, it is currently very difficult to create legal instruments to force suspects to provide the law enforcement with keys. This is mainly due to civil rights issues, and ultimately it is up to the owner as to whether they want to decrypt the data.

Another issue encountered during the Silk Road investigation involves the legality of remote searches in terms of the techniques used and the transnational authority of warrants. A remote search involves government hackers gaining remote access to machines, bypassing the requirement of physical seizure. As of now, the legality of remote searches varies by country. Law in Canada extends search warrants to all data stored digitally in the area of the search. Transnational regulations raise further issues. Extending search warrants beyond state boundaries to hack foreign computers opens up serious privacy and abuse of power concerns. Only rarely do law enforcement agencies have the authorization to do this. Therefore, the author believes multinational task forces and international cooperation will have to increase.

Finally, the author discusses the involvement of intelligence agencies in the fight against cybercrime through an analysis of the documents released by whistleblower Edward Snowden. He notes that SIGINT agencies have more sophisticated resources, expertise and technical means than civilian law enforcement. These resources are often aimed at targeting foreign threads and terrorist activity, and are far too secretive and intrusive for domestic law enforcement. Yet, with the amount of recent publicity received by these intelligence agencies and their advanced capabilities, the author foresees that their involvement in law enforcement operations may increase in the near future. Accordingly, such a case will require more detailed regulations regarding the authorization of their use against domestic targets.

Bojarski, K. (2015). "Dealer, hacker, lawyer, spy. Modern techniques and legal boundaries of counter-cybercrime operations." *The European Review of Organised Crime. 2*(2), pp. 25–50.

THE STRUCTURE OF QUEBEC'S SYNTHETIC DRUG MARKET

A competitive synthetic drug market exists in Quebec

The synthetic drug market in Canada has been at the forefront of recent law enforcement agendas and has received heightened media attention. This is mainly due to several large border seizures and reports published by narcotics bodies emphasizing the immense size of this drug market. Synthetic drugs are man-made drugs produced via chemical synthesis, such as ecstasy (MDMA), synthetic marijuana, and bath salts. Few studies have examined the structural elements of synthetic drug markets, especially in Canada. Disagreement exists over whether this market is controlled by a few large, highly organized illicit enterprises, or whether it consists of mostly small criminal groups that are competitive and transient. This lack of insight primarily stems from the methodological difficulties inherent to studies of hidden and secretive markets, particularly the problem of accessing reliable study participants. As such, researchers have developed innovative approaches to study the synthetic drug market and analyze its structure.

The following article is one such example. The authors conducted a drug composition and economic analysis using seized drugs and price data in Quebec. Drug composition analysis can tell researchers about the market through the chemical makeup of the drug (e.g. composition of substance) and its physical properties (e.g. colour and logo). When producing synthetic drugs, there are a wide range of synthesis methods and an endless amount of possible colours and logos. Linking drugs by similar characteristics can provide knowledge about the number and size of drug manufacturers in a given area. Economic analysis using price data can reveal the economic factors at work in the market.

The first stage of the study involved a descriptive overview of the market through drug composition data. 365 synthetic drugs were obtained from seizures made by law enforcement agencies in nine different areas of Quebec between June 2007 and 2008. These were

analyzed and classified by chemical composition and physical properties by Health Canada. It was found that the tablets had a wide range of different chemical compositions and physical properties. Price data was also obtained from the seizures. The majority of the drugs were sold as "speed" (67%) and prices were found to closely resemble those reported in other Western countries.

In the second stage, a network analysis was performed using the same data. This technique enabled researchers to uncover the "ties" between the seized drugs in regards to chemical composition and physical properties. It was found that the most popular tablet contained methamphetamine and caffeine (27% of all seized drugs). Only 43% of drugs sold as ecstasy and 66% of drugs sold as speed contained the active substance they were being sold as. It was discovered that a high variability of chemical and physical features existed between the seized drugs, with only 13% of drugs possessing identical characteristics with one or more tablets.

To statistically model the relationship found in the network analysis, a cluster analysis was conducted. The researchers regrouped the chemicals based on purity and assimilated them into larger categories (Grade A, B and C) to ensure the reliability of the test. Physical logos and colours with a sufficient number of cases (n=3) were included as variables. Once variables were grouped into clusters, ANOVA tests were conducted to provide a portrait of price determinants at the provincial level and in regards to drug prices in Montreal compared to other geographic locations.

The most important findings from this study are: First, a high number of different drugs were found in the sample. The authors claim this provides evidence of multiple synthetic drug producers in Quebec operating in a competitive market. Second, the drug's composition and whether it is sold as ecstasy or speed influenced its price, depending on the region. Prices in Montreal were only influenced by whether the drug was marked as speed or ecstasy, while outside of Montreal they were only influenced by quality of the drug. The authors note that this is likely due to market structure and production costs. Outside of Montreal, traffickers likely sell by quality to increase trust and future sales. Within the urban setting of Montreal, traffickers are unlikely to need to develop a strong consumer base through trusting relationships due to a higher number of potential clientele.

Several limitations to this study must be noted. Logos on drugs can be forged to associate the drug with a high quality brand. Researchers could have mistakenly classified drugs with the same logo as originating from the same manufacturer. Also, the researchers were unable to acquire information on the concentration of each substance. It was assumed that drugs with the same chemical composition came from the same production batch, while different quantities of the substance would indicate multiple manufacturers. Finally, this study operates on the assumption that manufacturers consistently use the same method and recipe. This assumption has not been confirmed by the literature. The authors point out that if this is not the case, they could have overlooked a single producer altering their manufacturing process.

Ouellet, M., & Morselli, C. (2014). "Precursors and Prices: Structuring the Quebec Synthetic Drug Market." *Journal of Drug Issues, 44*(1), pp. 37-55.

UNDERSTANDING THE DEVELOPMENT OF ILLEGAL ENTERPRISES

The logistical demands of an illegal operation dictate the size and structure of the enterprise

This article examines the relationship between the scale and modus operandi of illegal operations and the size of criminal enterprises. It contributes to the ongoing debate regarding the constraints that illegality imposes on the development and growth of organizations involved with the sale of illegal goods and services. Existing literature has argued that a trade-off exists between security and efficiency. This means that illegal enterprises can gain greater profit with bigger size, but at the cost of increased risks of detection and disruption. It has also been argued that large illegal enterprises are in a better position to deal with these risks because of a pooling of assets, recruiting dispensable individuals for hazardous tasks, or recruiting individuals for specialized tasks such as security purposes. Another proposition poses that illegal enterprises gradually progress along a pathway from small, individual groups to large organizations, changing with the nature of crime they commit.

This article contributes to the dialogue on the relationship between the scale of operation,

organizational size, and risk-minimization through an analysis of illegal enterprises involved in the cigarette black market in Germany from 1990 to 1999. The study is focused in the Berlin area, which had the highest geographical concentration of contraband cigarettes. During this time period, the illegal cigarette market operated through various schemes. For instance, one scheme involved genuine brand cigarettes being diverted from legal distribution channels in other countries and then smuggled into the German black market.

Data was collected from the German Customs Service data base (called INZOLL) and criminal files accessed through the Berlin prosecutor's office. INZOLL stores data on cigarette-related investigations, and information for this study included the number of seized cigarettes and the number of suspects in cigarette related cases. Case files from INZOLL were also used in this study for case studies into those that had the most complex and thoroughly investigated offender structures in order to gain insight into the operation of some of the key players in the Berlin cigarette black market. The criminal files comprehensively document all the evidence that has been collected and reviewed during the course of an investigation, along with subsequent court proceedings.

In terms of the scale of operation, the INZOLL data was classified into three categories: small (less than 50,000 cigarettes seized), medium (50,000 to 250,000 cigarettes seized), and large scale (more than 250,000 cigarettes seized). The vast majority of cases (97.9%) fell into the first category, however, considerable variation in the scales of operations was apparent. Most operations (91.6%) involved only one registered suspect, with the largest amount of suspects involved in a single case being 17.

Looking at the criminal files of 69 illegal operations with at least two individuals engaging in a criminal endeavour, most cases were found to be small-scale operations. The author classified his findings into a three-fold typology. First, "self-sufficient illegal enterprises" were the most common. These are mainly small-scale operations that do not draw on any outside support beyond their social networks. Second, "semi-integrated illegal enterprises" drew on external support (e.g. renting vehicles) as private citizens or under the guise of small, non-trade related businesses. Finally, "integrated illegal enterprises" were organizations also integrated into legitimate business processes. Their main source of security was their ability to blend into the legal economy, often through the operation of front companies.

Overall, the authors discovered that the illegal market they examined tended to be populated by small scale operations. At the same time, a relatively small number of large scale operations accounted for a substantial portion of the illegal activity. They found that operations that handled large amounts of contraband cigarettes tended to be larger in size. Furthermore, these large enterprises had a greater horizontal and vertical differentiation than those operating at a smaller scale. Finally, it was found that smugglers often extend their activities into legal spheres.

von Lampe, K. (2015). "Big business: Scale of operation, organizational size, and the level of integration into the legal economy as key parameters for understanding the development of illegal enterprises." *Trends in Organized Crime*, 18, pp. 289-310.

For more information on research at the Community Safety and Countering Crime Branch, Public Safety Canada, to get a copy of the full research report, or to be placed on our distribution list, please contact:

Research Division
Public Safety Canada
340 Laurier Avenue West
Ottawa, Ontario K1A 0P8
PS.CSCCBResearch-RechercheSSCRC.SP@canada.ca

Research Highlights are produced for the Community Safety and Countering Crime Branch, Public Safety Canada. The summary herein reflects interpretations of the report authors' findings and do not necessarily reflect those of the Department of Public Safety Canada.

ISSN: 2369-8144