Transnational Crime and Canadian Criminal Intelligence

https://www.e-ir.info/2009/12/16/transnational-crime-and-canadian-criminal-intelligence/

PAUL KNIGHT, DEC 16 2009

Abstract

The discipline of criminal intelligence must increasingly address the strategic threat of serious and organized crime, utilizing new resources, partnerships, and methods to combat the spread of international criminality. Crime in the 21st century poses a major asymmetric threat to Canadian society, demanding enforcement that is flexible, responsive, and grounded in defensible strategic goals. This will require solutions beyond standard bureaucratic shifts, necessitating a broad change in organizational mindsets and shifting the emphasis of enforcement from a tactical "statistics-based policing" model to a more strategic, long-term approach. Some strategic innovations in criminal intelligence may include the expanded use of joint force operations (JFOs), financial intelligence (FININT), open source intelligence (OSINT), and shared intelligence databases. Without ongoing support to criminal intelligence and the analysts – both uniformed and civilian – who conduct it, the nexus between organized crime, terrorism, illicit trafficking, and fragile states will continue to foment global instability.

Criminal and Strategic Intelligence: An Introduction

Criminal intelligence is the result of analysis on criminals and crime data, whether at a tactical (e.g. burglaries on Yonge Street), operational (e.g. homicides in Alberta), or strategic level (e.g. Canadian heroin trafficking). Criminal intelligence as a final product can take many different forms: mapping of crimes, statistical analysis of crimes, critical assessment of enforcement options, predictive analysis of crime trends, criminal network analysis, or written reports on criminal individuals and enterprises. Criminal intelligence is used in support of investigations into criminal activities, generally aimed at enforcement and prosecution under the relevant legal statutes. One already begins to see significant differences between criminal intelligence and national security intelligence; while the former is often aimed at supporting *enforcement* activities and may be submitted as evidence during legal proceedings, the latter is frequently generated in support of *monitoring* or *disruption* activities taking place outside policing and judicial systems. Additionally, criminal intelligence is generally not applied to terrorism, espionage, or sabotage, all of which remain in the sphere of national security intelligence. In the post-9/11 Canadian context, while the Canadian Security Intelligence Service (CSIS) has maintained some small degree of involvement with issues of transnational organized crime, this field is primarily the responsibility of the Royal Canadian Mounted Police (RCMP), the Criminal Intelligence Service of Canada (CISC), and relevant provincial/municipal police departments. In summary, criminal intelligence is concerned primarily with "identifying, prioritizing, and intervening" against criminal activities with the objective of "minimizing risk" to law-abiding society.

Strategic intelligence constitutes the process of strategic analysis and the resulting product of*analyzed information which is applicable at a strategic level*. Information is collected, under the broad guidance of policymakers, and subsequently analyzed. This process of analysis transforms strategic-level information, such as statistics on the Chinese armed forces, into strategic-level intelligence, such as the relative *capabilities* of the Chinese armed forces relative to NATO forces. Strategic intelligence informs policymakers at the highest level of decision-making, providing the basis for decisions which might have ramifications on the national or international stage. Because the 'customers' of strategic intelligence are frequently the senior members of a government or agency, the final product of strategic intelligence analysis generally must be concise, informative, and written in plain language. In the Canadian context, one of the primary producers of strategic intelligence is the Privy Council Office's International

Assessment Staff (IAS), which provides senior Canadian officials with strategic assessments of developments at a national and international level. IAS collates large amounts of raw data and intelligence produced by the broader Canadian intelligence community (IC), further packaging and analysing it for strategic-level consumption. IAS also maintains relations with Canada's international partners in intelligence assessment. IAS is thus an excellent example of a strategic intelligence producer, since it generates high-level intelligence, operates in close proximity to senior policymakers, collates intelligence from numerous operational and tactical-level sources, and maintains relations with international partners in the field.

Strategic intelligence analysis, in the context of criminal intelligence, will become an increasingly necessary feature of law enforcement. Strategic analysis may be applied in this field when assessing issues of national and international importance, whether they involve transnational organized crime, international drug trafficking, international human trafficking, or complex fraud. With the onset of globalization, organized crime has increased in sophistication and international connectivity, leading the to term "transnational organized crime". Transnational organized crime focuses on "sophisticated frauds, schemes, and thefts, involving both illicit as well as legitimate commodities, all operating according to market principles that ensure a profit".[1] Transnational organized crime also works to exploit international price differentials in both licit and illicit materials, trafficking in drugs, persons, cigarettes, antiquities, counterfeit goods, and numerous other commodities. These networks are both fluid and sophisticated, incorporating Old World criminal structures (Triads, Cosa Nostra, et al.) and increasingly entrepreneurial individuals without such affiliations. These international networks undermine the laws of their various host nations, denying billions of dollars of tax revenues that would otherwise flow to the state. Transnational organized crime also undermines the border integrity of host nations, undermining national sovereignty and potentially damaging trade relations with neighbouring countries.

Crime as a Strategic-level Threat

Contrasted with terrorism – the post-9/11 issue *du jour* — organized crime inflicts far more grievous damage upon states, depriving them of revenue and spreading drugs, prostitution, and violence to a degree with which terrorism seldom compares. Organized crime may also exert a corrupting effect on its host societies, working to influence officials to aid in the commission of large-scale criminal acts. In some cases we have witnessed the "criminalization" of broad sectors of society; in Russia, "systemic exploitation"[2] by organized crime has entered the world of both business and politics. In Brazil, organized crime operating out of the prison system has gained unprecedented strength, orchestrating a wave of attacks in May 2006 which resulted in over 400 deaths and brought entire cities to a standstill.[3] Today Mexico remains in a state very near civil war, as drug cartels vie for the domination of entire cities. Indeed, new reports are concluding that crime – especially organized crime and its trafficking activities – is increasingly correlated with civil warfare and state fragility.[4] To counter these trends before they reach such a critical level, enforcement activities must move beyond individual persons and individual networks, operating a broader strategic level of analysis to counter a strategic level of threat. Resulting enforcement activities, supported by strategic criminal intelligence, could include internationally-coordinated stings on criminal networks, simultaneously striking network 'hubs' and 'spokes' across international borders. These efforts must recognize the increasingly globalized nature of crime and the 21st century reality of a 'flat' world. This new paradigm, which criminal intelligence must address, is characterized by rapidly spreading instability unconstrained by the existence of oceans or borders.

Some responses to transnational organized crime have been truly international in scope, due in part to the heavy international focus on serious and organized crime during the 1990s.[5] In 2000 the United Nations' Office on Drugs and Crime (UNODC) drafted the Palermo Convention Against Transnational Organized Crime, which placed special emphasis on human trafficking and migrant smuggling. The Palermo Convention recognized the widespread existence of transnational organized crime, recommending cooperation between national enforcement bodies, increased sharing of intelligence, and the establishment of financial intelligence units (e.g. FINTRAC in Canada) to counter fraud and money laundering.[6] The Convention also sought to ease criminal property seizure[7] reduce bank secrecy,[8] improve cooperation on extradition,[9] and establish channels for mutual legal assistance.[10] The Convention even goes so far as to recommend state support of specific investigative techniques, including electronic surveillance and undercover operations.[11] All of the aforementioned measures could greatly facilitate a strategic-level approach to criminal intelligence, particularly in combating organized crime. To counter international networks, it

is clear that international cooperation is necessary. The Palermo Convention thus set out the groundwork for international strategic intelligence sharing in support of transnational organized crime investigations. These proposed measures may alleviate some of the difficulties inherent in combating these networks; however, the inevitable non-compliance of certain nations will continue to frustrate these efforts, as criminal enterprises will continue to base themselves in the world's 'zones of least resistance', sometimes known as "black holes",[12] where authority is most corrupt or diffuse.

Strategic intelligence analysis, operating at an international level, will clearly be necessary to confront transnational organized crime. Numerous threats have emerged, and will continue to emerge, with implications for Canadian law and order. Asian organized crime, such as the Triad societies and Japanese Yakuza, enjoy "global relationships" that yield "real potential to become… formidable threats to Canada and the United States".[13] Eastern European organized crime (EEOC) has, since the disintegration of the Soviet Union, matured into "fully realized transnational organized crime syndicates".[14] In the case of the YBM Magnex fraud, Russian mafia members carried out a massive international financial scheme with a Canadian component; stock market manipulation was conducted by using a Canadian stock exchange "to legitimize the criminal organization… whose assets [had] been artificially inflated by the introduction of proceeds of crime".[15] Italian organized crime (IOC), once at the brink of collapse after numerous successful RICO prosecutions in the United States, has re-emerged with new vitality in the 21st century. Their connections extend across the world, including to Canada, where most Sicilian IOC continues to be based in Montreal. Outlaw motorcycle gangs, such as the Hell's Angels, have also proved particularly apt at achieving near monopolies on drug trafficking, particularly in certain Canadian provinces such as Ontario and Quebec. All of these diverse networks require different and innovative approaches to enforcement which must be supported by strong intelligence analysis; by incorporating high quality, target-centric analysis, enforcement agencies can maximize efficiency by selecting high impact targets for investigation and prosecution. This, in turn, may lead to strategic-level improvements in combating organized crime.

Strategic analysis may also recommend enforcement and investigative strategies, generally based on empirical analysis of what has previously achieved success. In order to achieve a strategic advantage, it is necessary to move beyond traditional approaches of 'statistics-based policing', which determines success based solely on numerical results (e.g. kilos of drugs seized). This will require sound advice from analysts, who may recommend longer-term strategies, such as the use of confidential informants, wiretaps, or joint-force operations (JFOs) in coordination with other agencies. Analysts are in an ideal position to recommend such actions, given their strategic overview of the enforcement environment; police officers, by contrast, will often be focused solely on the present case at hand, too busy to occupy themselves with a "big picture" approach. An overarching strategic mindset, methodically working to dismantle broader criminal networks, will likely have far greater success than a narrow approach. Target-centric analysis, combined with warning analysis, could ideally recommend *when* and *whom* to target for investigation, grounding these recommendations in a set of strategic objectives. Target centric analysis will often recommend enforcement actions against members of a network with the highest connectivity (i.e. links to other network 'nodes') and specialization (i.e. they are difficult to replace). Successful actions against such targets can severely disrupt the organizations within which they operate; eliminating key individuals can thereby multiply the effects of enforcement. These key individuals are, additionally, often high-ranking members of their criminal organizations, whose prosecution can possibly lead to plea bargains which in turn implicate other high-ranking members.

Recent work in Canadian strategic criminal intelligence has met with great success, as displayed by the recent conclusion of the RCMP's Project SPAWN which begun in January 2007. SPAWN analyzed 793 law enforcement files dating from January 2005 to August 2007, scanning for data relevant to criminal activity at airports.[16] This review was augmented by interviews and site visits to all 8 of Canada's Class 1 international airports. Based on the strategic study, 58 organized crime groups were identified with links to Canada's major airports, 32 of which had facilitated their trafficking activities through the corruption of airport employees. This represented a significant minority of the 230 organized crime groups involved in transnational smuggling activities.[17] SPAWN also identified 1,326 individuals related to airport trafficking, 298 of which were airport employees, of which a "majority"[18] were still employed at Class 1 airports. This study therefore collated useful data on a strategic threat to Canadian society, in the form of international trafficking activities frequently occurring with the involvement of corrupted airport employees. The project also opened up significant venues for further investigation by authorities such as the Canada

Air Transport Security Agency (CATSA), the Department of Transport and the Canada Border Service Agency., Moreover, due to the issuing of an unclassified version, Project SPAWN generally increased public and governmental awareness of this critical issue.

Strategic Approaches to Criminal Intelligence: The SLEIPNIR Methodology

The RCMP has increasingly turned towards strategic intelligence and intelligence-led enforcement, moving away from its previous paradigm of "community-oriented policing". This new paradigm appears to have fit well with the organization, leading to an increased tempo of policing and a number of key strategic initiatives. One of these initiatives has been the SLEIPNIR threat assessment methodology, which attempts to categorize organized crime groups based on their current level of threat to Canadian society. The level of threat is assessed through 19 criteria, all of which are assigned a value – either "unknown" or from "nil" to "high" — based on their observed magnitude (see Annex I). These criteria address both the capabilities and qualities of criminal organizations. Some key capabilities include: violence, corruption, infiltration, subversion, specialized expertise, and the use of intelligence. Qualities of these organizations include: stability, mobility, scope, group cohesiveness, and discipline. All of these criteria are in turn weighted based on their perceived strategic significance, with corruption, violence, and infiltration, respectively claiming the highest level of significance. This is based in turn on the assumption that political corruption and criminal infiltration of government pose the highest strategic threat to Canadian society, threatening to undermine the fabric of Canadian law, order, and good governance. Each of these capabilities and qualities is further defined in order to precisely assess its strategic significance; for example, a "high" level of violence is defined as violence which is pre-meditated, calculated, and has a small likelihood of successfully being prosecuted.[19]

The precision and depth of SLEIPNIR allows for rigorous strategic analysis to be applied to criminal intelligence, assessing the overall risk to Canadian society posed by the approximately 971 organized crime groups within its midst.[20] This in turn permits enforcement strategies that are based on observed levels of threat and risk, as opposed to the political or bureaucratic whims at any given moment. The continued tracking of criminal entities through SLEIPNIR also allows for temporal strategic analysis of Canadian organized crime, from which trends and emerging issues in Canadian criminality can be observed. The SLEIPNIR methodology is, however, necessarily grounded in certain assumptions. One such assumption is that organized crime groups with connections to "criminal extremist groups" (e.g. terrorists) do not necessarily pose the highest level of threat; indeed, "connections to criminal extremists groups" is the lowest-weighted attribute in the SLEIPNIR system. This may not reflect the increasingly disturbing linkages between organized criminals and terrorists; for example, Mexican drug cartels have at times cooperated with Hizballah,[21] while South African and Armenian criminals were found to be "ready to sell… a range of sophisticated military-grade Russian weapons" and possibly even "enriched uranium" to NYPD officers posing as terrorists. Surprisingly, the second lowest-ranked SLEIPNIR attribute is "connections to other organized crime groups"[22]. This low emphasis on interconnectivity, combined with the relatively high emphasis on corruption and infiltration, would lead in turn to a certain set of strategic priorities. Such priorities might lead to a myopic focus on large, sophisticated groups, while ignoring the presence of small, cohesive groups with potentially dangerous connections to terrorism or foreign organized crime. This may result in highly ambitious targeting, focusing enforcement activities on groups which are too large to completely dismantle, thereby overlooking more easily disrupted "targets of opportunity".

Regardless of some (likely necessary) assumptions, SLEIPNIR nonetheless contributes to a nuanced strategic approach to criminal intelligence, helping to set enforcement priorities based on observed evidence, threat, and risk. Its ongoing application also allows for future scenario analysis and trend prediction, further highlighting its strategic applicability in the long-term. Given the increasingly widespread deployment of SLEIPNIR by the Canadian enforcement community, it provides the additional strategic advantage of determining "priority organized crime group threats"[23] for the entire Canadian policing community.

SLEIPNIR and similar methods can be used to fulfill the primary goal of strategic intelligence, which is to provide "some form of foreknowledge"[24] to policymakers regarding both ongoing and potential threats, in addition to the enforcement strategies deployed against them. The multi-year data produced by SLEIPNIR-type methods further permits robust, empirical analysis. One such example is Time Series analysis, which is a "powerful tool for evaluating

the effectiveness of a response"[25] by policymakers or enforcement agencies. Time series analysis allows one to separate natural fluctuations in a problem (e.g. seasonal shifts) from the results of an implemented policy (e.g. increased sentences for gang-related activities). The longer the time frame analyzed, the greater confidence one can gain from their conclusions. SLEIPNIR, with its time-series charting of organized crime capabilities, will allow for such rigorous empirical analysis, permitting Canadian authorities to observe their fight against organized crime from a long-term, strategic perspective. Time series analysis is, however, a complex method, and this form of strategic intelligence analysis might therefore necessitate the employment of statisticians, economists, or other experts in manipulating multi-year data.

Strategic Approaches to Criminal Intelligence: Joint Force Operations

Another ongoing initiative in criminal intelligence is the use of joint forces operations (JFOs), involving "multi-agency coordination and cooperation".[26] This strategic response has been popular in both Europe and North America, after the issuing of the 1997 European *Action Plan to Combat Organized Crime*, which recommended both "national level" bodies and "multidisciplinary integrated teams" to combat organized crime.[27] Robert Fahlman, RCMP's Director General of Criminal Intelligence Program Development, advocates "maximum collaboration"[28] not only between law enforcement authorities, but also extending to the wider sphere of academia and private industry. This collaboration is intended to address the "matrix of new challenges"[29] posed by transnational crime. However, despite such recommendations and an "almost universal"[30] belief that national security and organized crime threats must be met with a coordinated, "whole-of-government" response, the successful use of JFOs has nonetheless been a very challenging goal. Numerous inhibiting factors exist, including institutional rivalries, jurisdictional boundaries, differing mandates, 'stovepiping', and poor communication.[31] Canada has nonetheless attempted to make use of JFOs, beginning in 1970 with the creation of the Criminal Intelligence Service Canada (CISC), designed to facilitate cooperation on intelligence issues among member agencies. The goals of CISC are far-ranging, including the coordination of intelligence "collection, collation, evaluation, analysis, and dissemination,"[32] achieved through the use of the Automated Criminal Intelligence Information System (ACIIS) operated by the agency. CISC generally employs seconded personnel from member agencies, further contributing to the goal of integrated enforcement.

JFO approaches to criminal intelligence are clearly necessary, as criminal enforcement necessarily involves the contribution of federal, provincial, and municipal authorities. Like the field of national security, with its 'information silos' of HUMINT, SIGINT, and other forms of intelligence, criminal enforcement involves a large number of member agencies. JFOs appear to have been chosen as the strategic response to major criminal issues in Canadian society, and like SLEIPNIR, member organizations of varying jurisdictions and sizes have chosen to participate.[33] Some strategically-oriented JFO approaches have included the RCMP-led Integrated Proceeds of Crime (IPOC) units, the Sûrete du Quebec-led 'Project Wolverine' (which successfully aimed at ending the mid-nineties biker wars in Quebec), and the US-Canadian Integrated Border Enforcement Teams (IBET) which incorporates members of RCMP, CBSA, and US Customs and Border Protection. These JFOs aimed at criminal enforcement have mirrored the Canadian national security approach, which has involved Integrated National Security Enforcement Teams (INSETs) and an Integrated Threat Assessment Center (ITAC), aimed at bringing together national security agencies such as CSIS, RCMP, CSE, and CBSA. Future JFO initiatives could even move to a higher, international strategic plane, incorporating regional and international policing organizations such as Europol and Interpol. On a more tactical level, certain RCMP systems such as the Violent Crime Linkage System (ViCLAS) work to "encourage and facilitates communication between investigators"[34] tasked with investigating violent crimes which may be related; this in turn may facilitate a tactical JFO, including members of diverse police agencies.

Despite ambitious goals, Canadian JFOs have at times failed in providing support to *all* of their participants; generally, leading members of JFOs (often the RCMP) have reported higher levels of satisfaction with JFO results.[35] Members of leading agencies generally ranked their JFOs higher in terms of their effectiveness, significance, and contribution to the achievement of agency mandates. Unfortunately, subsidiary agency respondents noted high levels of dissatisfaction in terms of JFO intelligence gathering, analysis and sharing;[36] this demonstrates that JFOs have yet to achieve the strategic goals of all their member agencies, instead favouring the enforcement objectives of the leading participants.

Key Issues in Criminal Intelligence

Some ongoing issues may prevent the widespread use of criminal intelligence analysis. Without such broad-based support, JFO operations and national databases such as ACIIS may find limited success, thus undermining strategic coordination and success. Criminal intelligence analysts are frequently civilian members of their respective forces, which can lead to tension between uniformed members and their civilian colleagues. Some analysts believe that, without previous policing experience, they would find themselves lacking credibility in the eyes of their uniformed colleagues.[37] Indeed, some police officers are "very biased against civilian staff in general,"[38] feeling that their lack of policing experience renders their analytical insights suspect. Police officers often feel "uncomfortable accepting recommendations from non-police personnel" for fear it might "encroach upon their role".[39] These biases must be overcome in the Canadian policing community, particularly at the municipal level, in order for criminal intelligence to achieve its appropriate role and its concomitant strategic impact. While the author's interviews with civilian members of RCMP have indicated a high level of acceptance for civilian analysts, it appears that municipal and provincial agencies are not equally welcoming. The Ottawa Police currently employ only one civilian analyst in its intelligence section, who in fact only works on part-time basis.[40] While 'intelligence-led policing' is increasingly lauded as the new enforcement paradigm, intelligence branches in municipal and provincial police forces have remained relatively stagnant, whereas the RCMP Criminal Intelligence section is in its second year of a seven year expansion phase. Thus, while analyst hiring and civilian acceptance may be growing in Canada's federal police agency, it remains to be seen whether similar trends may emerge in provincial and municipal enforcement. Without a community-wide acceptance of criminal intelligence analysis – which is often carried out by civilians – it is unlikely that criminal intelligence will lead to strategic coordination across jurisdictions. In the absence of such coordination, it is unlikely that criminal intelligence will achieve any macro-level successes against the myriad issues facing Canadian society.

With an increasingly vast array of enforcement issues at hand, including "arms trafficking, identity theft, environmental crime, money laundering, theft of cultural property, drug trafficking, crimes against women and children, organ trafficking"[41] and cybercrime, it is increasingly clear that coordinated, strategic criminal intelligence must be employed, bringing together diverse agencies and employees in the fight against serious and organized crime. Cybercrime, especially, will only continue to increase as globalization fosters higher levels of digital interconnectivity. Canada, with its advanced high-tech industry and widespread internet connectivity, may prove to be a favourite target of criminals operating in cyberspace. These numerous issues will require creative and continually evolving solutions from the field of criminal intelligence and enforcement, which must necessarily move beyond traditional remedies and temporary stopgap measures.

What may *not* achieve success is the creation of new "super agencies", such as the U.S. Department of Homeland Security (DHS) and its Canadian counterpart Public Safety and Emergency Preparedness Canada (PSEPC). These agencies represent the common government response to new issues: bureaucratic organizational change. This approach is "unlikely to work in most cases,"[42] particularly in the absence of innovative new methods and policies. The mere shifting of organization charts is unlikely achieve strategic success against organized crime, it simply creates a more rigid, hierarchical, multi-tiered organizational structure. Such structures are poorly matched against the constantly evolving, asymmetric threats posed by serious and organized crime. In the Canadian case, PSEPC is also completely devoid of a strategic analytical function, instead focusing entirely on policy analysis and advocacy; this results in a lack of high-level analytical coordination, as may be found at DHS. Thus, more useful organizational changes might include increased authority for middle-management, enabling "imaginative, flexible, and lateral"[43] cooperation and innovation. Moreover, while a policy-oriented "super agency" may be appropriate for overseeing the work of national security agencies such as CSIS, its work sometimes overlaps with that of RCMP, which already possesses a robust policymaking capability. It is therefore imperative that new policies and JFOs are built "around existing institutions and their people,"[44] as opposed to the approach of layering additional bureaucratic structures upon existing institutions.

Analytical products must also be accepted and utilized in order to prove useful; the analytical products of criminal intelligence are too often perceived as "window dressing" or "wallpaper" and "ignored when planning [enforcement] operations".[45] Intelligence products are instead misused on a *post hoc* basis, merely to "summarize… outcomes

or… justify an operation that was already planned".[46] This is an excellent example of the "tyranny of the tactical," which focuses entirely on operational concerns to the often detrimental exclusion of strategic goals and perspectives. This problem may be ameliorated by the use of systems such as ACIIS, wherein analytical products are integrated with the everyday tools of policing. Such databases also eliminate some psychological barriers to officer-analyst interactions, as they may reduce the need for officers to personally consult with civilian analysts (and thereby admit that their role may be useful). Other databases, such as *i2 Analyst Notebook*, provide a fairly user-friendly, graphical interface for both analysts and officers to consult. With contributions from both civilian and uniformed members, such databases can become an digital medium that facilitates cooperation, collaboration, and the sharing of information. Nonetheless, no database or software will entirely ameliorate officer-analyst tensions, and enforcement agencies should therefore inculcate the belief that criminal intelligence is a core component of intelligence-led policing.

Policy Recommendations for Strategic Criminal Intelligence

Many ongoing policies and institutions in Canadian criminal intelligence make a contribution to strategic analysis and should therefore be continued. CISC has proven especially valuable, incorporating members from diverse agencies and creating databases with widespread access and applicability. CISC also produces lengthy strategic assessments as well as shorter assessments on new, relevant issues (e.g. pharmaceutical counterfeiting). These help to continually alert the enforcement community to emerging issues, in addition to providing a regular update on statistics and trends in Canadian criminality. CISC and the spirit of intelligence sharing which it represents is extremely valuable, offering value to the entire Canadian law enforcement community and bolstering the capability of small police forces through their access to this powerful intelligence network. The expansion of the RCMP Criminal Intelligence section is another valuable initiative which will free up time for analysts to work on strategic issues; if only a few analysts were available, day-to-day tactical issues would tend to dominate their busy agenda. Another positive development has been the SLEIPNIR methodology, which increases strategic analytical rigor. The creation of an OSINT unit within the RCMP has also been beneficial, allowing investigators to task OSINT collectors with targets which are in turn researched through numerous OSINT sources; in the future, such groups should be emulated throughout Canadian law enforcement and national security. All of the aforementioned developments – particularly taken as a whole — are sufficient to create a strategic advantage for Canadian criminal intelligence in its asymmetric conflict with serious and organized crime.

In terms of JFO initiatives, it may be beneficial to increase the role of the Integrated Threat Assessment Centre (ITAC) in criminal intelligence. Because serious and organized crime poses a major threat to Canadian society, ITAC could be tasked with the broad dissemination of knowledge on criminal issues throughout Canadian government; compared to ITAC, the circulation of CISC documents within the government is relatively limited. International partnerships should also be fostered, as groups such as INTERPOL have been left to languish in recent years (although a new director at INTERPOL has proven a valuable champion of its role). Canadian cooperation with the International Criminal Court (ICC) could be explored as well, although this nascent judiciary body is unlikely to have a strategic effect on Canadian criminality. In summary, if Canadian criminal intelligence bodies seek to recognize and address the reality of *transnational* crime, they must also operate and cooperate in a *transnational* context.

Although it is merely one of many threats, cybercrime will increasingly emerge as a danger to Canadian society which could rapidly attain a strategic level of significance. Canada is at present the most highly connected country in the world,[47] yet awareness of cyber vulnerabilities is "still in its infancy".[48] Phishing, malware, botnets, identity theft and viruses are only some of the many dangers inherent in the digital age, and will continue to affect Canadians. Many of the perpetrators are and will continue to be based beyond Canadian borders, making chances of prosecution minimal in the absence of international cooperation. Cybercrime, as a potentially low cost, high value form of criminality, will continue to expand and pose an increasing threat to Canadian servers in the possession of individuals, businesses, and government. Criminals are already exploiting these vulnerabilities, causing up to $10 billion in losses globally in 2009.[49] To address the emerging strategic threat posed by the intermingling of cybercrime and organized crime, Canadian authorities – including CSIS, CSE, and particularly RCMP – should actively participate in bilateral and multilateral initiatives to combat this rising threat. One possible avenue could be increased Canadian collaboration with IMPACT, the intelligence sharing and crime tracking branch of the International Telecommunication Union.[50]

One emerging front in combating serious and organized crime is the analysis and dissemination of financial intelligence (FININT). Under its obligations within the Financial Action Task Force (FATF), for which Canada assumed a one-year presidency in 2008, Canadian authorities have significantly expanded their FININT capabilities. The primary Canadian FININT institution, the Financial Transactions and Reports Analysis Centre (FINTRAC), has seen steadily increasing resources and an expanding mandate, in addition to powerful new enabling legislation. Because of the significant liaison capabilities inherent in the mandate of FINTRAC, including the ability to disclose information to CSIS, RCMP, CSE, and the Canada Revenue Agency (CRA), FININT is in a position to become a valuable strategic weapon against organized crime. By tracking the byzantine movement of funds, sometimes between many banking institutions located across the globe, FININT disclosed to RCMP may help to illuminate the reach and depth of Canadian organized crime. This in turn will open up new avenues for investigation and prosecution. Such intelligence sharing will only become more necessary as organized crime finds new niches for financial exploitation, such as the rising use of mortgage fraud, already creating losses ranging into the "hundreds of millions annually".[51] The use of FININT is absolutely necessary, given estimates that money laundering accounts for between 2% and 10% of the global GDP, totalling between $800 billion to $4 trillion dollars *per annum*.[52]

Unfortunately, money laundering and financial fraud (i.e. "white collar" crime) cases remain complex and difficult to prosecute, often requiring specialists in forensic auditing and other uncommon fields of expertise. Therefore, in the foreseeable future, it will remain common for Canadian Crown Prosecutors to arraign professional criminals on charges related to violence or drug trafficking. Unfortunately, strategic success may be difficult to achieve in this regard, as high level criminals are rarely directly implicated in such activities. Strategic progress against crime syndicates may therefore result only when FININT is deployed against the elite of organized crime; while this may be costly and lengthy, it is preferable to the alternative of continued low-level, ineffectual prosecution of insignificant criminal "soldiers". Increased FININT capabilities must be pursued if authorities are to confront the rise of flexible criminal syndicates which increasingly "need to move capital, set up and liquidate companies, circulate money, and invest quickly… without geographical restrictions".[53]

Conclusion

It is imperative that Canadian authorities in criminal intelligence move to combat serious and organized crime, which increasingly posed a strategic threat to Canada, its international partners, and indeed the global community. By utilizing new resources, partnerships, and method, the present asymmetric advantage afforded to organized crime may be reduced. In the future, "intelligence led policing" must be based on defensible strategic goals, pursued through a whole of government approach, combining the advantages of uniformed and civilian analysts. This will at times prove difficult, as it will require a difficult evolution in organizational mindsets, moving the present model of enforcement to a more strategic, long-term basis. The may be facilitated by greater use of joint force operations (JFOs), financial intelligence (FININT), open source intelligence (OSINT), and broadly accessible digital intelligence. These measures must be combined with international cooperation aimed at dismantling international criminal syndicates at multiple "hubs"; to do so, new partnerships with sometimes reticent partners (e.g. China or Russia) must be forged. Other partnerships, including those with private industry, academia, and the general public, should be continually cultivated to ensure their contributions to criminal intelligence are heard. Conversely, some problems to be avoided include process of intelligence 'stovepiping', overclassification of criminal intelligence data, the creation of bloated "super agencies", conflicting mandates among competing authorities, and unequal power distribution within JFOs.

If Canadian authorities in criminal intelligence are to seriously address the strategic threat posed by serious and organized crime, they must utilize their growing resources in an efficient, effective, and innovative manner, constantly utilizing empirical methods – such as SLEIPNIR – to assess ongoing policies and progress. The sweeping recommendations of the Palermo Convention, while ambitious, could provide a strong general framework for the development of Canadian criminal intelligence and its international partnerships. International warning and communication systems, such as those maintained by INTERPOL, should be fostered and expanded, working to globalize both raw intelligence and professional analytical assessments. As modern crime has grown into a borderless, networked system, so too must criminal intelligence agencies strive to mirror their opponents, working towards rapid interchanges of intelligence, coordinated enforcement responses and unified strategic objectives.

[1] Margaret Beare. *Structures, Strategies, and Tactics of Transnational Criminal Organizations: Critical Issues for Enforcement*. Transnational Crime Conference, Canberra, March 9-10, 2000.

[2] Beare. *Structures, Strategies, and Tactics of Transnational Criminal Organizations: Critical Issues for Enforcement*.

[3] Sergio Adorno and Fernando Salla. *Organized Criminality in prisons and the attacks of the PCC*. http://www.iea.usp.br/iea/english/journal/61/adornosalla.pdf.

[4] The SecDev Group. *Armed Violence Reduction: Enabling Development*. http://www.secdev.ca/Secdev-temp/Publications.html.

[5] James Sheptycki. *Organizational Pathologies in Police Intelligence Systems.* European Journal of Criminology, Vol. 1(3), p. 308.

[6] *United Nations Convention against Transnational Organized Crime.* Article 7.1b. http://www.uncjin.org/Documents/Conventions/dcatoc/final_documents_2/convention_eng.pdf.

[7] *Ibid.* Article 12.3-4.

[8] *Ibid.* Article 12.6.

[9] *Ibid.* Article 16.

[10] *Ibid.* Article 18.3.

[11] *Ibid.* Article 20.1.

[12] Moises Naim. *Illicit,* p. 262. Random House, New York: 2005.

[13] Criminal Intelligence Service Canada. *2006 Canada/US Organized Crime Threat Assessment*. 2006.

[14] *Ibid.*

[15] Margaret Beare. *Russian (Eastern European) Organized Crime Around the Globe*. Transnational Crime Conference, Canberra, March 9-10, 2000.

[16] Royal Canadian Mounted Police. *Project SPAWN,* p. 1. http://www.primetimecrime.com/Recent/Organized%20Crime/projectspawn.pdf.

[17] *Ibid.* p. 9.

[18] Royal Canadian Mounted Police. *Project SPAWN,* p. 3.

[19] Steven J. Sang. *Project SLEIPNIR: An Analytical Technique for Operational Priority Setting,* p. 2. https://analysis.mitre.org/proceedings/Final_Papers_Files/135_Camera_Ready_Paper.pdf.

[20] Royal Canadian Mounted Police. *Project SPAWN,* p. 3.

[21] Naim. *Illicit,* p. 137.

[22] *Ibid, p. 262.*

[23] Robert Fahlman (Director General, Criminal Intelligence Program Development). Personal interview, March 2009. See Annex I.

[24] Thomas Quiggin. *Seeing the Invisible: National Security in an Uncertain Age* , p. 185. World Scientific, London: 2007.

[25] Ronald Clarke and John Eck. *Crime Analysis for Problem Solvers*. www.popcenter.org/learning/60Steps/.

[26] Stephen Schneider and Christine Hurst. *Obstacles to an integrated, joint forces approach to organized crime enforcement,* p. 308. Policing, Vol. 31(3), 2008.

[27] *Ibid.*

[28] Robert Fahlman. Personal interview.

[29] *Ibid.*

[30] *Ibid.*

[31] *Ibid.*

[32] Schneider and Hurst, p. 311.

[33] Robert Fahlman. Personal interview.

[34] RCMP. *Violent Crime Linkage System (ViCLAS)*.http://www.rcmp-grc.gc.ca/tops-opst/viclas-salvac-eng.htm.

[35] Schneider and Hurst, p. 315.

[36] Schneider and Hurst, p. 311.

[37] Nina Cope. *Intelligence led Policing or Policing led Intelligence?* British Journal of Criminology, 44(2), p. 190.

[38] *Ibid.*

[39] Cope. *Intelligence led Policing or Policing led Intelligence?*, p. 191.

[40] Thomas Quiggin. Personal Interview, March 2009.

[41] Robert Fahlman. Personal interview.

[42] Sir Richard Dearlove and Thomas Quiggin. *The Tyranny of the Tactical*. http://dr.ntu.edu.sg/bitstream/10220/4305/1/RSIS-COMMENT_444.pdf.

[43] Dearlove and Quiggin. *The Tyranny of the Tactical*.

[44] *Ibid.*

[45] Cope. *Intelligence led Policing or Policing led Intelligence?*, p. 192.

[46] *Ibid*.

[47] Internet World Statistics. http://www.internetworldstats.com/am/ca.htm.

[48] The SecDev Group. *Tracking Ghostnet*. http://www.scribd.com/doc/13731776/Tracking-GhostNet-Investigating-a-Cyber-Espionage-Network.

[49] The SecDev Group. *Tracking Ghostnet*.

[50] *Ibid*.

[51] Criminal Intelligence Service Canada. *Mortgage Fraud and Organized Crime in Canada*. November 2007.

[52] Naim. *Illicit,* p. 137.

[53] Robert Saviano. *Gomorrah: A Personal Journey into the Violent International Empire of Naples' Organized Crime System*. Trans. Virginia Jewiss. Picador, New York: 2007.

Annex I: Unclassified SLEIPNIR Group Capability Matrix

Source: "Project SLEIPNIR: An Analytical Technique for

Operational Priority Setting"

Annex II: Interview with Mr. Robert Fahlman

Q.#1: Do you believe that transnational organized crime constitutes a significant, "strategic" threat to Canadian society?

A. #1: Transnational organized crime either of itself, or linked to international terrorism, poses a matrix of new challenges to both law enforcement and security intelligence agencies alike, in Canada and at a global level.
The "business" of organized crime takes in illicit profits estimated at

US $1,000 billion annually (United Nations, 1996). As seen on the international stage, increasingly networked, techno-savvy OC groups have the capacity to corrupt individuals, government and indeed nations fueled by the vast profits realized by illicit activities including arms trafficking, identity theft, environmental crime, money laundering, theft of cultural property, drug trafficking, crimes against women and children, crime over the Internet and trafficking in body parts. These challenges, often daunting, require maximum collaboration between law enforcement agencies as well as with government at all levels, private industry and academe – both domestically and internationally.

Q.#2: Do you believe the role of Criminal Intelligence in Canadian police work is expanding, contracting, or remaining constant?
A. #2: The role of criminal intelligence is definitely expanding in Canada as well as at the international level. Post 9-11 has seen a significant increase in criminal intelligence resources, largely due to the realization that intelligence provides the most effective "early warning" apparatus to deal with critical threats, known and unknown, whether criminal or terrorist in origin.

Q.#3: How valuable is the role of Criminal Intelligence Analysis in the context of policing transnational organized crime?
A. #3: Criminal intelligence is an indispensable tool in policing international organized crime. For the same reasons noted in combating crime at the domestic level, crime at the transnational level demands that law enforcement work collaboratively at the international level. The enhanced intelligence capacity of regional and international policing organizations such as Europol (European Union) and Interpol (global), clearly underlines the key role and value played by criminal intelligence at the macro level.

Q.#4: How successful have the RCMP's attempts at Threat and Risk Assessment (e.g. SLEIPNIR) been? Are these assessments integrated with the operations and priorities of RCMP?

A. #4: The RCMP Threat Measurement Tool known as SLEIPNIR has been invaluable in establishing a common threat measurement standard for the RCMP which has since been endorsed and applied by the wider law enforcement community. CISC for example applies SLEIPNIR in its integrated Provincial and National Threat Assessments on Organized Crime. Both internally within the RCMP and within the wider CISC community, this tool assists in determining priority organized crime group threats for the Canadian law enforcement community.

—

Written by: Paul Knight
Written at: Norman Paterson School of International Affairs, Carleton University, Ottawa Written For: Prof. Thomas Quiggin Date Written: April 1, 2009