

The Criminal LAWYER

No. 163 June 2006

Contents

- 1 The Charge of Arson
- 3 The Law of Unintended Consequences – a Perspective on the Draft Directive on Criminal Measures to Enforce Intellectual Property Rights
- 5 Intercountry or Transnational Organised Crimes
- 8 Notes

Subscription inquiries: Tel: 01444 416119
e-mail: customerservices@tottelpublishing.com

Editor: Andy Sinclair LLM
e-mail: TheCriminalLawyer@lycos.com

© 2005 Tottel Publishing ISSN 0956 7429

Tottel
publishing



Intercountry or Transnational Organised Crimes

Sally Ramage

Transnational organised crime¹ presents interesting dilemmas for law enforcement agencies. The most significant problems facing law enforcement agencies have to do with both the nature of transnational organised criminal activity, which closely resembles white-collar crime, and the structure of relationships between law enforcement agencies as they attempt to combat complex economic crime across jurisdictions. The first step in addressing transnational organised crime is to acquire a thorough understanding of

the technology of offending and the nature of and mechanisms for reducing regulatory conflict between law enforcement agencies at the various levels of government.

Local Law Enforcement

To understand the issues facing local law enforcement as it attempts to deal with transnational crime, we must under-

¹ The most important authority is the United Nations Convention against Transnational Organised Crime and its Protocols 2000

stand the advances in rapid transit and information systems that have led to the globalization of crime. In the UK, there is the Serious Organised Crime and Police Act 2005, which, it is hoped, will curb the steady progress made by organised criminals into the United Kingdom.

Such local law enforcement faces much more basic and mundane problems that affect its ability to respond to transnational crimes. Because of this, transnational crime poses unique and important problems to local law enforcement thanks to the permutations of crime and social control which are products of different cultures, legal structures, and systems of enforcement.

Local law enforcement is not well situated to effectively respond to offences that are technologically or organisationally complex. One reason for this inability is that local law enforcement has as its primary goal, to respond rapidly and reactively to citizens in need. Meeting this need alone strains local law enforcement resources to the limit.

The nature of organised and white-collar crimes requires an inter-organisational response from law enforcement. There are significant regulatory conflicts of interest. In order to frame an understanding and response to transnational crime at the local level, the nature of these crimes needs an examination. To establish some basics, we must accept that a transnational crime is any crime because it merely becomes transnational simply by the offender travelling to another country.

The nature of organised crime and white-collar crime

Definitions of organised and white-collar crime have been provided by Geis, 1992; and Helmkamp, Ball, & Townsend, 1996; Kelly in 1986; Schragger & Short, 1978 and so on. What is meant by organised and white-collar crime for the purposes of this analysis? White-collar crime is understood here as illegal behaviour governed by criminal statutes committed by individuals or organisations in the course of their legitimate economic activity. Organised crime is defined here as illegal behaviour governed by criminal statutes committed by organised groups of individuals for the purposes of supplying illegal goods and services.

The National White-Collar Crime Center estimated in 1996 that US annual losses from white-collar crime to range from 260 billion to 1 trillion dollars US. Today, worldwide, this would amount to trillions of US dollars. However, it is the permutations of organised crime that worries law enforcement.

The old maxim of "follow the money" is as true today as in ages past. If you want to understand white-collar crime, follow the money. Transnational crime has become the problem it is, because the social organisation of money has itself become transnational. This is the nature of business activity as it seeks to maximize profits and the mechanisms or technology available to make it possible. The patterns of white-collar crime reveal a move to the use of computers due to the development of computers and information technology, and to securities and commodities, banking, and insurance, telemarketing, instant electronic transfers, because global communication via the Internet has become normal business practice.. At the same time, there are now many satellite centres that service these

new activities, these being large brokerage firms, health organisations, law firms, and international accountants.

White-collar crimes are evident in these service centres due to the trust that is inherent in their fiduciary roles as agents. White-collar and organised crime often intersect at this point, as organised criminals seek ways of moving and hiding money and goods and turn to these specialized functions to facilitate their financial crimes.

Law enforcement agencies face this complexity and have to deal with the harm that transnational crimes produce. Harm entails both the injury caused by the crime, and the intent of the criminal. White-collar crime poses particular problems because of the injury and the victims it creates. Injury such as physical well-being and economic security as well as damage to democracy and market confidence.

When injury is direct, people understand crime better. Because they can see the effect on specific individual welfare interests White-collar crime however causes injury that is more diffuse Securities frauds of the may be spread over a large number of victims, many of whom may not be people at all , but institutional investors .

The second component of harm is intent

Intent is perhaps most significant because it affects both the perception of victimization, which initiates the degree of culpability and the criminal remedy

A key aspect of white-collar crime is that it thrives on the opportunity structures created when white-collar crime mimics legitimate behaviour and then it is most difficult to enforce against. How many people today can say that they understand the 1980s Milken fraud that led to front page stories on most major newspapers and magazines?

Regulatory conflict arises with respect to the remedial jurisdiction of much of the illegal economic activity. The focus of law enforcement is the establishment of criminal intent, and this becomes difficult when either the activity approximates acceptable activity or the means to engage in the illegal activity are themselves legal as in the wiring of money to offshore accounts.

The intent- offence

The component of intent is closely tied to another feature of many white-collar offences. The idea that white-collar offences are particularly complex has been the subject of considerable academic debate. There is a hierarchy of white-collar offences that is based, in part, on offence complexity.

Research on white collar crime mostly concentrates on individuals acting in their occupational roles - there has been little on the organisation of crime. All crime is socially organised in some way or other, and organised transnational crimes are embedded within the formal and informal organisations of various complexity.

Organisational complexity is a function of the parts of the organisation and of the criminals and their position within the organisation. Its structure and function, include the formal and informal operating policies, task specializations, communication and decision-making systems, and organisational culture and norms. Increasing evidence suggests that many types of organisations and organised crimes are better depicted as taking place within networks of individuals and groups.

Networks of organised crimes

These networks expand and contract according to the particular criminal opportunities that are available and take on their own complexities. This makes it harder for law enforcement to develop any systematic response due to these criminals' fluid and dynamic nature. Networks form and disband, acting in many ways like a cancer invading the body. They change in response to the conditions in the environment and to the reactions of the host. As soon as law enforcement begins to understand the structure and activities of the network, the network alters its shape or changes its direction. These criminal organisations consist of sets, some more complicated than others. Their sizes and ability and the way specific criminals work are crucial factors that law enforcement need to study.

Core Technology of Organised Crime

Organisational complexity is embedded in the organisation itself; it can also be thriving because of its specific core technology. Organisations involved in white-collar crime function for the specific purpose of completing particular tasks because those tasks are established in the context of legal behaviour.

It is crucial to determine the degree of organisational criminality (as opposed to individual criminality), and this can be a particularly daunting task for law enforcement when the behaviour takes place in the context of legitimate activity within complex market or industrial systems. Technological complexity is the defining component of the most serious forms of white-collar crime.

Temporal and spatial complexities

Finally, temporal and spatial complexities are key components to many forms of organised and white-collar crime. It is seldom the case that organisations that move illicit goods or provide illegal services are geographically centralized, and many forms of white-collar crime evolve out of special circumstances and conditions that blend over time to create the right opportunity structures. Organised and white-collar crimes have some unique features. There is a dearth of information available on country and local responses to white-collar crime.

Local law enforcement constraints

Local law enforcement can do little more than respond in piecemeal fashion to random complaints that are filtered their way. They are ill equipped to develop systematic and structured mechanisms whereby cases are prioritized, delegated, and managed. Local law enforcement lacks the resources and personnel to respond to sophisticated cases that are organisationally or technologically complex

Disadvantages and advantages in having task forces

One solution to these concerns is to develop multi-agency task forces. These task forces can take a variety of forms, but they typically involve some formalized relationships between agencies with specific agreements that pertain to a specific case or type of crime.

Such task forces, as the UK Serious Fraud Office and the UK's Serious and Organised Crime Agency, can be seen by some as a drain on already limited time and resources.

Unless there is some direct benefit from their participation, many see task force participation as energy that could be spent more effectively on other matters. Unless there is a steady flow of important and solvable cases that focus attention and provide a set of common problems to work on and to create a specialist database.

Most of those who work in the field of national or international financial services regulation would agree that the compilation of a database covering global financial services regulators, supported by extensive explanations of the financial services regulatory structure in 105 jurisdictions round the world, was an ambitious task.

The difficulties of tackling securities fraud

A web site for an illegitimate company can be created using the same graphics, icons, and font type as those used by a respected and trusted company. The use of symbols laden with familiarity and repute lends legitimacy to information placed on the imitating pages. Deception is possible because the symbols that represent a trusted company are no more "real" than the symbols that are reproduced for a fictitious company.

Both are intangible and both involve the intent and effect of evoking trust. Relationships between symbols and meanings, which have been established through experiences in the physical world become destabilised in an Internet environment.

A modern securities transaction,

The process of exchange in a securities transaction is often nonmaterial, entirely electronic, with a digital transfer of money from one account to another. In addition, it is a digital entry assigning ownership to a specific number of shares. When transactions involving non-physical property are conducted in an environment where user identities and locations are elusive, where the currency of exchange is symbolic and where the target population is millions of people opportunities for deception are extraordinary. This is the problem of internet securities regulation.

Legal dynamics of the internet that facilitates organised crimes

Technical governance of the Internet, or the development and maintenance of Internet protocol, has been in place since 1979, when the Internet Configuration Control Board (ICCB) was established. However, this form of governance was not designed for legal or social issues concerning the Internet community; it was designed to support the technical evolution of the network. This utopian perspective is intimately related to and functionally protected by the First Amendment in the United States.² Efforts to legislate restrictive measures for Internet communication or heighten surveillance of Internet activities, for instance; have been confronted with argu-

2 The First Amendment to the US Constitution – Freedom of rights, Press, Expression, ratified 15th December 1791. "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances."

ments alleging violations of at least the First Amendment, and often the Fourth Amendment,³ and the Privacy Act and the Electronic Communications Privacy Act.

Traditional regulation cannot cope with the internet

Traditional forms of regulation are defined by geographic and functional jurisdiction.⁴ The former has been completely defied by Internet technologies; yet, regulatory "authority" is still largely restricted by geographic boundaries. This imbalance has served as a catalyst for communication among regulators. However, where communication has not been adopted as a norm, deterrence has become more difficult

Regulation on an international level has been proposed as an alternative that could resolve jurisdictional barriers. However, it seems both unlikely and infeasible (technically, legally, and politically) for regulatory responsibility involving multiple countries to be assumed by any international agency. Currently, the International Organisation of Securities Commission (IOSCO) is involved in the co-ordination of inter-national agency efforts and communication. Direct regulatory authority by the OSCO, on the other hand, would undoubtedly require the normalization of numerous diverse laws, rules and norms and a substantial degree of restrictive controls.

Internet securities fraud

Internet securities fraud is possible not only because of knowledge of Internet technologies but also because of the ability to construct false information around the image of an investment. Constructed information is used to manipulate perceptions and responses of potential investors. However, all Internet communications generate power-knowledge. Therefore, knowledge about the general methods of fraud, particular fraudulent events, and verified corporate activities can render the knowledge that is created by violators less valuable to victims. Power created by alliances, then, may define knowledge or truth.

Internet groups

Examples of power-knowledge effect are found throughout the Internet. Over the past several years, many websites have been developed for the purpose of gathering and disseminating information about fraud, some examples of which are Crime Prevention and Criminal Justice, the Centre for Strategic and International Studies, Convention Against Transnational Organised Crime and the Nathanson Centre on Organised Crime websites.

Others include the Cyber Angels, a site that is headed by a former member of the Guardian Angels and is entirely non-governmental. This site follows a model that is similar to self-governance, with internal networks such as Angel Buddies, Net Patrol, and various chat rooms. Cyber Criminals Most Wanted and The Internet Fraud Council are also privately organised, whereas sites that involve both governmental and non-governmental participants include the "International Web Police".

Regulatory agencies and other governmental agencies, which have enormous information resources and capacities, can promote activities that inform individuals, directly and through groups. Government can publish easy to read articles explaining the investigatory powers of the Director of Public Prosecutions, for instance. How many people in the UK understand how these powers work? How many would know that, in connection with the investigation of offences of organised crimes in the UK, the DPP may delegate the exercise of his powers to a Crown Prosecutor; or that the Director of Revenue and Customs Prosecutions may delegate his powers to a Revenue and Customs Prosecutor? An authorised person may take copies of or extracts from any documents produced in compliance with a disclosure notice? Or that a Justice of Peace⁵ may issue a warrant for an authorised person to enter and take possession of documents, computers, disks, even if a building is unoccupied or the occupier is temporarily absent? And that such documents may be retained for so long as the Investigatory Authority considers that it is necessary to retain it (rather than a copy of it)?⁶

*Sally Ramage, BA (Hons) MBA, LL.M, MAAT, MCMI
Visiting Lecturer, School of Legal Studies
University of Wolverhampton*

3 The Fourth Amendment to the US Constitution states: "Search and Seizure. The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."
4 In the UK there is the Prevention of Terrorism Act 2005 and the Interception of Communications Act 1985
5 JP's are immune for acts within jurisdictions and from certain acts beyond jurisdiction – see the Justices of the Peace Act 1979 ss. 44 and 45.
6 Serious Organised Crime and Police Act 2005 s.66(7)(a)