

# When economic crime becomes organized: the role of information technologies. A case study

(in *Current Issue in Criminal Justice - Journal of the Institute of Criminology*, University of Sidney, faculty of Law, Vol. 11, n. 3, March 2000)

Andrea Di Nicola\* and Alessandro Scartezzini\*\*

*“My ‘master’ works for a foreign government. Another member of the group now works for multinational companies involved in electronic espionage: they pay him for doing the same things for which they previously convicted him [...] because nowadays the power is information” (as quoted in Maserà 1999).*

*[Raoul Chiesa, Italian hacker convicted in Operation “Ice Trap”]*

## Introduction

This comment is based on the idea that economic crime is increasingly committed on an organized basis so that the boundary between economic crime and organized crime is disintegrating. The essential assumption of the comment is that information technology is one of the main factors influencing this process of organization in economic crime. Economic criminals need information technology in order to manage essential and valuable information. The likely consequence of the use of these new technologies is a modification in the way criminals behave and organize. To better develop this idea, this comment looks at a famous and recent Italian case of computer crime: Operation “Ice Trap”.

## Operation Ice Trap: An Interesting Case Study

It is now accepted that the globalisation of the market has introduced more, and new forms of opportunity for criminals (see Findlay, 1999). Globalisation has given those interested in fraud, for instance, the opportunity to act on an international level by taking advantage of the lack of regulations in the commercial and financial markets of some countries. They use the latest technologies to provide themselves with links between criminals all over the world without concrete need for physical contact. An example is the case of international fraud that was detected by the Italian Police in collaboration with investigative forces from other countries. The operation, called “Ice Trap”, led to the arrest of 6 people and seizures in many Italian cities, and one arrest by the Swiss police. Investigation started with a communication by *Unilever International*, a British commercial holding, claiming that hackers were spying on the activities of many of its firms by entering the computer system of its Italian affiliate through the “*Sprintel*” and the “*Itapac*” nets. These computer nets were also used as a way of communication between Italian criminals and their European and North American counterparts. The members of the organization also used the Bulletin Board System on the Internet to exchange messages and plan their illicit schemes. Credit cards pins and passwords were illegally gained from the electronic databases and used for virtual transactions unknown to the legitimate owners of the credit cards (Ascenzi 1996). The hackers involved in the fraud organized themselves as a very flexible group, with different roles and with a leader, connecting themselves only via computer networks. Their high technological skills empowered them to keep under control computer systems in different countries. Evidence of this was given by the American secret service and by the investigative forces in France and Italy (Serra, Strano 1997). This case, in 1995, together with many others which followed are increasingly worrying crime investigators in many European countries. It demonstrates how criminal

---

\* Researcher at TRANSCRIME, Research Group on Transnational Crime, University of Trento (Italy) and PhD candidate, Universities of Bari-Trento (Italy).

\*\* Researcher at TRANSCRIME, Research Group on Transnational Crime, University of Trento (Italy).

organizations can easily build international connections for the planning and the perpetration of crimes, with the use of new technical know-how and equipment.

These concerns are even more justified if you consider the fact that the arrests of the hackers in operation "Ice Trap" mainly resulted from traditional means of investigations, especially telephone tapping. It is clear that the perpetrators of high technology crime are well ahead of conventional crime investigation when it comes to the adoption and application of information technologies.

Despite this realisation, the "Ice Trap" operation was an important step in the fight against hackers in Italy. It was the first time in which the offenders - besides being convicted of specific computer-based offences - were sentenced for '*unlawful association to commit a crime*'<sup>1</sup>. This was made all the more remarkable because the offenders had organized themselves, without knowing the identity of each other, relying for their communication and enterprise solely on the help of computer connections. Four years later, these criminals have been released from jail and they have been able to find legitimate employment. The strange thing is that they participate in more or less the same information technology activities as they did before their arrest and trial, but now they do so "legally" for private and public institutions. As one of these hackers observed: - "information is power" -. So where is the borderline today between legal and illegal activities in the information war?

This Italian fraud case underlines the reality that economic criminals are getting organized around information exchange like never before, and reveals how computers help in the evolution of their enterprise. New and flexible forms of criminal organizations for economic crime are taking shape in the criminal arena.

### ***Economic Crime gets organised***

There has always been an intense debate in criminology on the definitions of economic and organized crime. An enormous body of literature points out the overlap between these two forms of criminal activity, trying to explain why, where and how they are both moving towards greater rationalization and organization (Savona 1990). Some authors have highlighted - though in different ways - that economic crime is a particular form of organized crime (Ruggiero 1996; Nelken 1997; Savona 1998). According to them, specialization, professionalism and organization characterize economic crime. The more complex the context in which criminals operate, the more professional experience they require and the broad organizational structures they need in order to commit their crimes. This is the reason why large-scale economic offences need organization: to better achieve their results and to reduce risks. Economic criminals need detailed information on laws, techniques and practices in order to assess opportunities and risk. They need to build networks of people and skills in order to achieve higher degrees of commercial competence which modern criminal enterprise requires.

What we are facing is the risk that this debate on economic and organized crime will result in a sterile discussion of dichotomies, unsupported by the analysis of the developments that are taking place in these two criminal environments. If we look at trends in economic crime - and the above case represents a good example - we discover that its evolution is tightly linked to the new features of the market, and information transfer in particular. This evolution leads economic crime towards new forms of organization, though perhaps quite different from those we were used to seeing in the analysis of traditional organized crime. They seem to be more flexible and short-term, built on professional networks. Nevertheless, we continue the analysis in terms of organization. One of the factors that pushes economic crime towards organization is the role that information plays in modern society.

### ***New Information Technologies in Organizing Economic Crime***

Information, defined as a set of relevant data, plays a key role in modern society. The market is increasingly based on a cash-less economic model and new types of money and transaction systems

---

<sup>1</sup> Article 416 of the Italian Criminal Code which punishes the 'unlawful association to commit a crime' states: "*When three or more persons associate to commit several crimes, those persons promoting, establishing or organising the said association shall be liable, for this sole offence, to imprisonment for 3 to 7 years. For the sole offence of participating in the said association, the punishment shall be imprisonment for 1 to 5 years [...]*".

have developed based on information transmission technologies. Information has become an essential and rare factor of production and its management has become the most important element in every decision process and every strategic business development.

Economic crime is influenced by this information revolution in two ways.

First, as a valuable and contained factor of production, information itself is a (direct or indirect) object of crimes committed by white-collar criminals. Information means profit. It can be a direct target when it represents the primary goal of an economic crime (ie. in industrial espionage). This was the case in operation "Ice Trap", which was a clear example of how economic crime focuses on stealing information, sabotage of information systems, and other criminal offences related to the security of information. Other examples where the information is the profit motive in crime are insider trading, industrial espionage, and the disguising of information. The strategic role for which information is increasingly acquiring leads to the commission of these crimes. Their perpetration depends on the intensive use of complex and sophisticated information technologies. Information can be an indirect target of white-collar criminals when it plays an essential role in the criminal organisation's "learning process". One imagines, for instance, the vast amount of information necessary to organise a large-scale fraud against the financial interests of the European Union. Knowledge in different areas - such as fiscal structures and strategies, customs regulations, industrial arrangements - is needed, together with the ability to collaborate around this knowledge, employing different languages and legislative backgrounds. In addition, corruption and other economic criminal behaviours are regularly reliant on information asymmetries and other information privileges. More generally, when criminals have to organise complex criminal schemes, they usually need to learn by acquiring detailed and diverse information.

The growing relevance of information has a second important influence on economic crimes. In order to commit them criminals need to adopt new instruments and new form of organization. Information is expensive and well protected. White-collar criminals know, because of their business background, that only with a flexible and organized structure it is possible to manage the complexity of information flow (United Press International, 1998; United States Department of the Treasury, 1998). For example, since valuable information is becoming more technical, specific and scattered all over the world, economic criminals are likely to develop a wide network in order to discover information and/or to sell it to the interested people. It is realistic to think that economic criminals will organize themselves adopting all those strategic information technologies useful in order to retrieve, manage and communicate important information. It's possible that white-collar criminals need to develop '*GroupWare capabilities*', as is the case in legitimate business parlance. It means that they will look for a group of technological instruments and organizational processes able to make the collaboration within flexible organizations easier and to improve the information management in non-formal organizational structures. The main aim of these technological and organizational innovations is to support complex processes, with large decision-making autonomy for its members, lack of rigid rules, with strong privacy concerns and with spatial and temporal challenges. They include all those technologies that can help the communication, co-ordination and collaboration with GroupWare, such as electronic message exchange, desktop conferencing, group decision support systems, and probably in future also artificial intelligence support. As reported in the main Italian bibliography about computerisation and business organizational issues, "GroupWare simultaneously represents a tool and a stimulus to sustain and develop new organizational strategies" (Filippazzi, Occhini 1993). This means that the adoption itself of these kinds of technologies will lead economic criminals to accentuate its non-conventional organization structure. Network organization, and occasionally joint ventures between criminals all around the world will probably be the most frequent form of aggregation, but supported by strong information management technologies. The overlap between legitimate and illegitimate market enterprise is also more and more likely, confusing the distinction between what is deviant, and what is good business.

## **Conclusion**

Today economic crime is characterized by the constant interrelation between legal and illegal activities. The presence of figures that do not belong to the typical criminal scene makes it complicated to recognize the borderline between the legal and illegal. In those criminal commercial contexts in which information plays a relevant role, it is also extremely difficult to distinguish between economic crime and

traditional organised crime. They increasingly have features in common. The distinction is becoming less viable.

First, both organised and economic crime emerge and flourish in a parasitic context, since they do not create added value and tend to infiltrate mainly those economic sectors they perceive to be highly remunerative. In other words, they infect and depend on legitimate market activities. Second, they rely on networks, with relevant contacts in the legitimate business. Third, they use specialist business and enterprise expertise in order to commit their illegal activities: they need professionalism and specialisation. Fourth, they tend to act rationally (certainly in a commercial sense), trying to weigh the benefits and risks of their illegal actions against market advantage and profit. Last, they adopt forms of organisational structure, even though the modalities in which they organise themselves are often extremely varied.

It must also be kept in mind, anyway, that these two kinds of criminality continue to display essential differences. Economic crime, unlike organised crime, does not request any bond of loyalty beyond normal commercial convenience. Traditional criminal values and forms of hierarchy in the structure of the organisation do not play as relevant role. Economic crime networks can work independently from ethnic or cultural proximity. The nature and identity of participants in the enterprise are less crucial issues. Economic crime, most of all, does not rely on enforcement through violence and intimidation. The question that arises, therefore, is why should economic criminals respect agreements among themselves? The answer is that the profit incentive behind continuous and ongoing crimes performed in association is of greater value than any anticipated benefit deriving from the breach of business arrangements and agreements. Technologies have a key role in this choice since through automation processes it makes it easier to repeat and continue the same criminal enterprise. Furthermore, economic crime is better facilitated than organised crime in the illegal management of information because of its professional background: the majority of the members of economic criminal organisations are likely to work in legitimate corporations in which information technologies are already highly developed.

The brief analysis of similarities and differences between organised and economic crime may be useful in identifying possible future strategies of action against new organised economic crime. The following are some suggestions in line with the comments made above. When investigating economic crime and devising counter strategies against new trends one should:

- try not to identify economic organized crime with traditional organizational structures (Mafia-type);
- consider as stable also the organization built up for a single illegal business;
- not look for traditional hierarchical structures, but concentrate on the identification of the real beneficiaries of crimes;
- realize the importance of information and evaluate the threat posed by an economic criminal organization especially on the base of its abilities of managing information;
- since the networks of economic criminals can be easily built up world-wide, develop countermeasures at the international level;
- better protect valuable information, using the best technologies in order to prevent and control economic crime.

The fight against economic crime, which is increasingly trafficking in information, can be won only through better management of information.

## **References**

Ascenzi, M.C. (1996) "Operazione Ice Trap", in *Polizia Moderna*, n. 3, pp. 14-15.

Filippazzi, F., Occhini, G. (1993), *Groupware*, Franco Angeli, Milan, p. 50.

Findlay, M. (1999) *The Globalisation of Crime*, Cambridge University Press, Cambridge

Masera, A. (1999) "Guardie e ladri", in *Panorama Web, Caccia agli hacker*, n. 4, Arnoldo Mondadori Editore, Milan, January [[http://www.mondadori.com/panorama/area\\_8/933\\_2.html](http://www.mondadori.com/panorama/area_8/933_2.html)].

- Nelken, D. (1997) "White-Collar Crime", in M. Maguire, R. Morgan, R. Reiner (eds), *The Oxford Handbook of Criminology*, Clarendon Press, Oxford, pp. 898-890.
- Ruggiero, V. (1996) *Economie sporche. L'impresa criminale in Europa*, Bollati Boringhieri, Turin.
- Savona, E.U. (1990) "Social Change, Organisation of Crime and Criminal Justice Systems", in U. Zvejkic, (ed.) *Essays on Crime and Development*, UNICRI, publication n. 36, Rome.
- Savona, E.U. (1998) "Economic Crime in Europe. Analysis of the Interdependencies among Fraud Money Laundering and Corruption", paper presented at the International Conference on *Economic Crime in Europe. Interdependencies among Fraud, Money Laundering and Corruption. Analysis and Responses*, Trento (Italy), 22-23 October.
- Serra, C., Strano, M. (1997) *Nuove frontiere della criminalità. La criminalità tecnologica*, Giuffrè, Milan, pp. 72-74.
- United Press International (1998) *High-tech crime now more 'flexible'*, Birmingham (England), 16 May
- United States Department of the Treasury, Fincen (1998) *Money in Cyberspace*, Washington [<http://www.ustreas.gov/fincen/cybpage.html>].