Security Sector Reform: Institutions, Society and Good Governance
Alan Bryden/Philipp Fluri (eds.)
Copyright © 2003 by Nomos Verlagsgesellschaft: Baden-Baden

Organized Crime, Terrorism and Cybercrime
pp. 303-312

Louise I. Shelley

The merger of transnational crime, terrorism and corruption is profound. The idea that these ideas can be discussed separately is problematic. Such compartmentalization limits our ability to analyze and address the diverse forms of transnational criminal activity. Highly corrupt societies give little opportunity for legitimate social mobility and their high level corruption is a deterrent to economic growth and investment. Under these circumstances, the employment opportunities of transnational crime groups provide a desirable economic alternative to youth without legitimate opportunities.[1] Terrorist groups flourish in environments where youths have limited chance for advancement within their societies.

The phenomena of transnational crime, terrorism and corruption are all too often viewed as separate phenomena. These phenomena have grown in tandem because the economic and political conditions that give rise to these phenomena are quite similar. The evolution of the transnational crime-ideologically based or economically based depends on specific environmental factors that have proliferated in many developing and transitional countries that have not successfully integrated into the global Economy.[2]

Terrorists and transnational criminals use many of the same strategies to promote their operations, chief among these being the use of information technology to plan and realize their activities.[3] The rise of greater international mobility and the proliferation of information technology throughout the world have facilitated the growth of both transnational crime and terrorism. The ease of communications in the contemporary era makes the location of groups and actors less significant than it was previously. The ability to exploit security holes in the system makes crime groups and terrorists operate out of unexpected locales rather than their home territories.

Most transnational crime and terrorist groups are based in transitional and developing countries. The illicit businesses are now the largest and most profitable to be located in the developing world. For example, the drug trade now represents about 7% of world trade according to late 1990s estimates of the United Nations.[4] Their vast profits and enormous assets make them powerful actors in their home countries and in their regions. Because they are so large relative to the legitimate businesses based in their region or in the countries through which they operate, they have a large influence on politics and business.

The vast profits of illegal businesses allow them to hire the best specialists domestically and internationally. Facilitating this trade, is an ever greater reliance on information technology to promote their activities secretly. For example, international **(End Page 303)** drug traffickers are among the most widespread users of encrypted messages, coded messages by cell and satellite phones and use anonymizer features on computers. They also are able to hire technical specialists capable of using steganography and other means to make messages hard or impossible to decipher.[5] This access to high level specialists allows illicit businesses and terrorist organizations to transcend borders and operate internationally without detection. Often the crime and terrorist groups do not need to go outside their region to hire such technical specialists. Some of the leading specialists in the technical area are located in regions that house major transnational crime groups and terrorist organizations.

The presence of many highly trained technical specialists in the countries of the former Soviet Union and in the Indian subcontinent means that transnational crime groups means that a vast array of specialists are available for hire.[6] While some specialists will not work for criminal or terrorist organizations willingly, some will do it unaware of their employers whereas others will agree to provide assistance because well-paid legitimate employment is scarce in their region.

The widespread problem of corruption in many developing countries allows the proliferation of transnational organized crime and terrorism. The official corruption facilitating this activity may assume many different forms and is not just based on bribery. Top government officials provide falsified documents to smuggled criminals and terrorists, restrain law enforcement from acting against suspicious groups and provide them a safe space to operate. Because of this, criminals can use the high level technology available in the former Soviet Union and the Punjab region to facilitate not only their own crime and terrorist groups but those of other regions of the world which find save haven on their territory. In this way criminals exploit information technology to carry on their operations in a safe and secure manner.

The connections between transnational crime and terrorism are not unique to developed and developing countries. As investigations in the advent of September, 11th have shown, terrorists in developed countries use criminal activity to survive. Arrests in Spain revealed that terrorists were selling counterfeit airline tickets to survive and such groups in the United States were surviving by means of money laundering and other criminal offenses.[7]

1 Organized Crime, Terrorism and Use of Information Technology

Technology links developed and developing regions by facilitating financing, rapid planning, and all forms of information sharing. Legitimate corporations have exploited the technological revolution to full advantage by use information technology to coordinate their international operations in developed and developing countries. This has helped them overcome problems of inefficient postal services, time differences among different regions and problems of international communication in a multi-lingual **(End Page 304)** environment. The linking of the developed and developing world in the technology area has provided financially beneficial to multinational corporations. They have been able to outsource work so that data processing and other information technology functions can be performed in regions with technical capacity but low labour costs.

Transnational criminal organizations, criminal and terrorist, also take advantage of the possibility of uniting the developed and developing country by information technology. Drug traffickers use encrypted messages to direct their operations.[8] Terrorists use the anonymizer feature of computers to coordinate their activities across countries. Websites facilitating all forms of transnational crime, for example dissemination of child pornography or recruitment sites for terrorist organizations, are often posted in developing countries without the law enforcement capacity to bring down these sites.[9]

Furthermore, law enforcement in these developed countries cannot hire or retain the personnel needed to combat the criminal activity of transnational crime groups. The low salaries and the corruption of law enforcement means that individuals with highly developed technical skills cannot find desirable employment in the state sector. Computer experts in developing countries choose not to work for low law enforcement salaries, instead they work for the private sector and others will work consciously or unknowingly for criminal and terrorist groups.

In some countries, even if the state paid adequate wages, the state law enforcement sector may not be a legitimate alternative to the criminal sector. The institutionalized corruption of much of law enforcement and its close links with the criminal sector in some regions of the world means that the criminals can pay for specialists within and outside the government.

In the developed countries, there is a shortage of personnel with adequate IT skills. Many of those who work in the high technology sector in Europe and the United States are immigrants from less developed countries and are not able to serve law enforcement in the countries in which they reside. Moreover, law enforcement has not been able to compete with the private sector in terms of the pay it offers or the promotional options which it provides to make it an employer of choice to talented IT specialists.

Criminals have been very successful in exploiting the international inconsistencies in the system and the failure to regulate technology across jurisdictions. As the love virus from the Philippines illustrates, there are limits on sanctioning offenders whose crimes are extremely costly to society because individual countries have not enacted legislation. While the perpetrator of the love virus did not intentionally cause the harm to computer systems around the world, individuals who intend to cause serious harm exploit the environments in which there is little regulation of computers and little law enforcement capacity to act against this crime.[10] One website containing child pornography was posted on a website indicating that it was located in a Central Asian country. Over four million individuals downloaded images from the site before it was brought down. The reason being is that there were an absence of computer specialists in that country to take down the website. **(End Page 305)**

The lack of coordinated legislation has been exploited not only by criminals but by terrorists as well. The hijackers of the September, 11th planes were aware that their phones and cell phones might be tapped. Before post-September, 11th legislative changes, separate warrants were needed to tap each phones in the three jurisdictions of the Washington area -- Virginia, Maryland and the District of Columbia. The terrorists exploited this knowledge of the limits of law enforcement and used different phones in these different jurisdictions to prevent monitoring of their conversations. Just as the future terrorists exploited jurisdictional differences in the Washington metropolitan area to reduce risk, they also did the same internationally.
Much of the plotting for the September, 11th attack was carried out in Germany that has the greatest limits on undercover activity. With its protections on the right to privacy and its limitations on police powers, a legacy of the abuses of the Nazi era, terrorists could use the advance telecommunications networks to their advantage without detection.[11] Intelligence and analysis by the terrorist cells helped ensure the ultimate security of operations with access to the most sophisticated information technology.

The merger of transnational organized crime with terrorism is seen on a regular basis. Terrorists use criminal activity to support their operations. The growth of information technology facilitates terrorists' attempts to gain significant profits with relatively low risk. Terrorists can finance their operations without resorting to violent assaults or bank robberies that would raise the risk of detection.

Criminal activity committed internationally via the Internet supports terrorist activity as they can tap into credit card bases and commit various forms of lucrative fraud. Ukrainian specialists at a TraCCC conference in 2000 reported that their country is the source of many financial crimes committed by computer and the Internet.[12] But while Ukraine may be the source country for much of this criminality, it is not now clear that only Ukrainians are committing this crime. There are many foreigners using the computer resources of Ukraine and they may be also contributing to this economic crime because they have identified this country as one with limited capacity to act against this crime. By means of corruption, they are able to obtain the right to reside and operate within the country.

Countries with high capacity in information technology and low capacity to act against crime committed using computers and telecommunications become havens for transnational crime and terrorism. The concept of a safe haven acquires a different concept when the weapon is not a conventional one but a piece of information technology which allows plotting, financing and possibly even executing a serious crime.

Information Technology is Central to Commission of Organized Crime and Terrorism

Before the advent of widespread information technology, the pace of international communications and transactions was slower. Secure measures of communications required trusted carriers, funds could be moved only slowly and planning across borders **(End Page 306)** was slow and laborious.[13] In the age of information technology, messages can be transmitted instantly without leaving a trace, massive wire fund transfers can occur across multiple jurisdictions in an hour and international plotting can occur within chat rooms and protected communications within a computer system. There has been a movement of money to areas where regulation is less. Even traditional systems of underground banking such as *hawala* or Chinese underground banking have been revolutionalized by the ability to provide almost instantaneous instructions on the delivery of funds.[14]

The criminal and terrorist exploitation of information technology has proceeded in tandem with its growth by the legitimate multinational community. In fact there is evidence that those who seek to promote illicit ends have been as fast if not faster to introduce this technology into their operations. The possibilities of introducing technology rapidly into transnational crime groups and terrorist organizations exists because the most modern organized crime groups and terrorist cells are organized as networks. Unlike the traditional mafia structure or the traditional top down corporation that react slowly to innovation, these new transnational criminal actors enjoy enormous flexibility. They have high level technical specialists within their organizations or employ the top specialists.

Both terrorists and transnational criminal organizations such as Colombian drug traffickers or Russian-speaking organized crime have used the full variety of information technology to achieve their desired results. This includes cell phones, satellite phones, computers, and virtual private networks. The latter are particularly valuable for undetected international operations.

Anonymity increases the difficulty of decoding encrypted messages. Both encryption and anonymizers are increasingly used by transnational crime groups. Once encrypted messages represented a very small share of the communications of transnational crime groups. But the use and the sophistication of the encryption have been increasingly exponentially. Therefore, increasingly messages are staying outside the capacity of law enforcement and the intelligence community to decipher. With the enhanced information gathering in the contemporary era, which law enforcement and intelligence cannot digest, those messages which are encrypted have even less chance of being incorporated into the analysis needed to address these groups.

Private safe, secure and rapid communications are key to the spread of organized and ideologically motivated transnational crime. The anonymity offered by computers in internet cafes and computer services allows criminal groups in many parts of the world to interact. Investigators found that terrorists in the United States used computers as Kinko's, a computer and copy store, to conduct their businesses. In other countries, millions have access to Internet through anonymous computers that sell their services by the hour. Without knowing the identity of those who use the computers and using constantly changing on-line addresses, messages are not traceable. Instant messenger provide the possibility of on-going interactive communication without leaving a trace that investigators can follow.[15] **(End Page 307)**

Information technology facilitates many aspects of the operation's of transnational crime groups and terrorists from their financing, to the documents that they need for their operations. The transnational illicit actors are able to produce fraudulent documents on the computer to provide them new identities, covers and to provide a paper trail which covers their operations. Human smugglers produce high-quality false identity papers for those who need new identities. These computer-produced documents may be of such high quality that their fraudulent nature is not discernable to even sophisticated law enforcement.

Computer systems help finance criminal and terrorist operations. The revolution in information technology has facilitated covert banking, more efficient underground banking, electronic fund transfers, and the use of debit and credit cards. Piracy and counterfeiting of goods, facilitated by information technology, is an important financial source for criminal groups. This is particularly true in the software area and other areas involving intellectual property. Criminals and terrorists can commit fraud on the Internet, can solicit banking information from gullible citizens, tap into insufficiently protected banks of credit card information or even tap into the online orders of some mail-order businesses. These are not hypotheticals but examples of the kind of financial activity used by these groups already detected by international law enforcers.

The logistics of transnational crime groups and terrorists are aided by information technology. The Internet aids the transport, tracking, monitoring and diversion of shipments. Part of the reason that drug traffickers can respond quickly to law enforcement crackdowns is that they monitor their shipments through elaborate computer systems. Identifying points of vulnerability, they are able to rapidly reroute their shipments to reduce the risk of intervention. Combing analysis with sophisticated computer programs, Colombian drug traffickers ensure that over sixty to seventy percent of drugs shipped enter the United States successfully.

Less covert means can be used by terrorist organizations that use the worldwide web to recruit and fund raise. Sites can be posted and taken down as needed. Therefore, they can reach a broad audience in many regions of the world. Those who are the most likely recruits for terrorist organizations are youthful males who are also the individuals in their countries most likely to have access to computers and the Internet. Therefore, investment in information technology provides a very valuable marketing tool to reach the most receptive audience.

2 Problems of Cooperation - Domestic and International

Many of the problems that impede transnational crime and terrorist investigations have already been cited. But examining them together reveals the fundamental challenges which exist in this age in which there are such discrepancies available to investigators and intelligence in the developed and developing and transitional worlds. Furthermore, the fact that the transnational groups have been among those to take most advantage of the globalized information system, highlights the very serious problems that exist in a world where laws are state-based and criminals and terrorists operate across many states simultaneously to carry out their activities.

The presence of so much of the information technology system in private hands and the presence of control over this system lying in state hands provides very serious **(End Page 308)** impediments to regulation and control.[16] The concept of public-private partnerships which exists in the United States is not an internationally recognized concept. It works haltingly in the United States and often proceeds only as an alternative to state intervention in the operations of Internet service providers (ISPs). Cooperation with law enforcement in pursuing purveyors of child pornography on the Internet is a preferential alternative for many ISPs rather than search warrants being issued to have access to their data bank.

Much tracking of crime committed over the Internet can be done by American law enforcement because so much Internet traffic is routed through the United States. But in traffic that does not pass through the U.S., the situation is more difficult. Different legal codes and procedures impede cooperation on the international levels. Many countries lack needed laws to address computer crime and crimes committed by means of information technology. Compounding the problem is that the global information infrastructure is outside the jurisdiction of anyone country.

Criminals and terrorists, as previously mentioned, exploit the weaknesses in laws and law enforcement capacity to execute their crimes. These are not casual decisions on how top operate effectively by computers but are instead based on calculations and careful training and analysis. The potential of the Internet is realized not only by the telecommunications industry but also by those who seek to foster their crimes and terrorist acts in effective ways.

3 Future Trends

Over the past years there has been a rise in the use of existing forms of carrying out covert operations by means of information technology. These include ever greater use of encryption, money transfer facilitated by computer system and increasing fraud over the internet. With the retention by top information technology specialists by transnational crime groups and terrorists, we can expect to see new and innovative uses of information technology by these groups.

Of greatest concern to many governments and international financial systems is the possibility of serious intrusions into critical systems. These intrusions could include the introduction of viruses that would destroy critical data, the posting of harmful websites that cannot be brought down and even the full scale incapacitation of critical computer systems.

The disruption of international financial markets remains a serious concern. The present interdependence of the world's economic system means that a disruption in one region of the world will have ripple effects in other regions. The constant monitoring of stock, bond and commodity markets by financial analysts world wide means that an intrusion and/or disruption of these systems would not go unnoticed. It would send shock waves outside of the market which is the source of the problem.

Money laundering is increasing with the amount of money outside regulated markets growing. This is a result of the growth of the illicit global economy that is supported by the profusion of offshore havens.[17] The proliferation of information technology increases the possibility of moving money covertly outside of any system of regulated **(End Page 309)** banking. Therefore, the recent crackdowns on the banking sector and The Patriot Act, which has ripple effects in international financial markets, means that illicit and terrorist money may increasingly be pushed outside the regulatory system. Movement of money through tangible commodities, businesses and *hawala* like currency transfers may be ever more possible because of the monitoring and facilitation of computer systems.

One distinct concern is that there will be more successful mergers and/or cooperation between organized criminal and terrorists in the information technology area. Cooperation between organized criminals and terrorists exists in Latin America, Europe, Asia and other regions of the world. Information technology expertise may be commissioned by one type of transnational criminal group and then subsequently exploited by another either for mutual advantage or as a business proposition.

Already there is enhanced exploitation of areas with sophisticated information technology and corrupt officials and corrupted and incapable law enforcement. This means, for example, that members of terrorist organizations can pay corrupt officials to obtain residence permits in a region where there is a high level of IT capacity. Then they can use the Internet resources or even finance their IT outlets and market them as public facilities. Incompetent law enforcement will not think to look at public Internet outlets as havens for terrorists. If they were to detect such a phenomena, they could be bribed to look the other way. In this way terrorists have secured a safe physical space but also a safe space in which to run their operations.

Enhanced mobilization and recruitment for terrorism by the Internet is an existing concern. This mobilization can be of funds and people. By using steganography, disclosing secret messages within other messages or pictures, communications can be made secretly to a large number of people. Without the linguistic capacity or the intelligence capacity to intervene in these groups, technology can be used to ever greater advantage.

Legitimate civil liberties concerns in many countries may curtail or limit monitoring of information technology. Because most information technology is controlled by the private sector, it is their primary concern to protect their customers rather than to counter transnational crime or terrorism. As cooperative as information technology companies may be, once a risk is defined, their initial interests are to make a profit rather than to prevent a crime or a terrorist act. The constitutional protections existing in countries which now enjoy information technology dominance place a premium on the privacy and rights of citizens. Therefore, the possibilities for information gathering are limited.

4 Tools to Respond

A strong dichotomy exists between the way states and multinational organizations respond to transnational crime and terrorism generally, and the particular threat posed by cybercrime committed by these groups. Because information technology is primarily in the private sector, public private partnerships are needed to locate abuse of the Internet by transnational criminals. This may include network monitoring by private corporations to detect suspicious websites or usage patterns.

The development of international teams of computer specialists incorporating information technology specialists from developing countries with advanced computer skills to work in cooperative ways to monitor transnational crime and terrorism. **(End Page 310)** International cooperation in a mutual process of information sharing is a key response to the problem.

There is a need to develop and support international security research teams with specialists from both developed and developing countries. There are a need for partnership relationships in which both parts of the team believe that it is in their interests to respond to any manifestations of transnational crime and terrorism that are evident through investigations of cybercrime. This may include a system of rewards that provide multinational incentives rather than those which are based on the country in which the investigation may occur. The rewards may be too low for the investigators and the chance of corruption may be too great.

There is a need for citizen assistance in identifying problematic and suspicious websites. Citizen support has been particularly valuable in identifying child pornography websites in the United States and in sites that are lures by human traffickers in Russia. In both of these countries, citizen groups have warned of abuses in order that Internet service providers can bring down these websites. This may not be possible in many situations where the citizens have sympathy with the goals and objectives of the terrorists but it can be most effectively done in cases of sexual exploitation, financial fraud on the Internet and potentially in relation to money laundering schemes on the Internet.

Penalties should be established for computer specialists who assist in international organized crime and terrorism. Just as the legal system has moved against lawyers and accountants and money launderers who serve criminals and terrorists, there needs to be the ability to readily prosecute the computer facilitators. There needs to be the harmonization of laws that individuals cannot operate out of safe havens which allow individuals to commit computer crimes without any risk of arrest and prosecution.

Investigations of the information technology component of the crime and the terrorist act must be an integral part of the overall investigation and not exclusively the domain of computer specialists. Coordination among citizens, private corporations, states and multinational organizations is central to addressing cybercrime that facilitates organized crime and terrorism.

5 Conclusion

Transnational criminals and terrorists have been major beneficiaries of globalization because they benefit from more open borders, greater international mobility and faster and more secure communications. Although the information technology revolution has provided the opportunities for greater access to information and democratization of societies, this development has benefited not only legitimate users but those which seek to harm others on the personal and political level.[18] International drug traffickers have exploited information technology to full advantage. They are not alone. Child pornographers and terrorists have exploited to this technology to their enormous advantage.

The expansion of international communications in the coming years will require much thinking on the appropriate balance between the protection of national security, the most effective means to protect the integrity of financial markets and of individuals **(End Page 311)** from fraudulent schemes or potential sexual exploitation. The ease and security with which transnational criminals and potential terrorists can transmit information, will provide a challenge in many areas that are not even foreseen at the present time.[19]

Even in countries that do not place a premium on privacy over national interest, like China, they cannot monitor the content of the messages which are communicating over their ever proliferating computer systems within their country. Therefore, the potential for abuse is even higher in societies that place a premium on free exchange of information.

The challenges to regulation are formidable. Telecommunications systems are often in private hands. Therefore, their control is outside of state authority. The concept of public-private partnerships is a concept alien to many states where the government is authoritarian, corrupt or infiltrated by organized crime. Compounding the problems is the lack of harmonization of laws dealing with the regulation of information technology. Even in the presence of laws, many countries do not have the law enforcement capacity or the even the computer equipment to adequately investigate the crime or detect threats to the system.

In contrast, in the United States, there is such formidable data collection from computer systems that analysts are unable to digest the information they possess. Therefore, there is a curious imbalance between the most technologically powerful country in the world that is overwhelmed with information and developing and transitional countries which cannot seek the information they need. This dichotomy between the most affluent and least affluent countries seen in many other areas of the contemporary world has startling consequences for the all the world.

The imbalance between too much information and too little, increases international political, financial and personal security. The full consequences of this will be seen in the coming years. **(End Page 312)**

Notes

1. For the link of corruption and organized crime see Sen, A.: "On Corruption and Organized Crime," in: *World Drug Report*. Oxford, Oxford University Press, 1997, pp. 150-153.
2. Farer, T.: "Conclusion Fighting Transnational Organized Crime: Measures Short of War," in: *Transnational Crime in the Americas*. Ed. Farer, T., New York and London, Routledge, 1999, pp. 244-52.
3. Shelley, L. and Picarelli, J.: "Methods Not Motives: Implications of International Organized Crime and Terrorism". *Police Practice and Research* (forthcoming).
4. United Nations International Drug Control Programme, *World Drug Report*. Oxford, Oxford University Press, 1997, p. 124.
5. Baugh, W.E. and Denning, D.E.: Encryption and Evolving Technologies: Tolls of Organized Crime and Terrorism. Excerpted in*: Trends in Organized Crime* 3. No. 1 (1997), pp. 85-90 as well as recent interview with DEA analyst.
6. See conference on *Transnational Crime, Corruption and Information Technology* sponsored by the Transnational Crime and Corruption Center, American University, Nov. 30-Dec. 1, 2000, www.american.edu/traccc.
7. “Eight Suspected in Aiding in Attacks are Ordered Jailed by Spanish Judge.” *Wall Street Journal*, 18 November 2001.

8. Freeh, L. J.: "Impact of Encryption on Law Enforcement and Public Safety". Statement before the U.S. Senate Committee on Commerce, Science and Transportation, Washington D.C., 19 March 1997, reprinted in: *Trends in Organized Crime* 3. No. 1, 1997, p. 93.
9. Hughes, D.: "Pimps and Predators on the Internet". 1999, www.uri.edi/dignity/Pubs.htm.
10. "Love Bug Bites UK", 4 May 2000, http://news.bbc.co.uk/l/hi/uk/736080.stm.
11. Marx, G. and Fijnaut, C. (eds.): *Undercover: Police Surveillance in Comparative Perspective*. Amsterdam, Kluwer, 1995.
12. See note 6 above for more detailed discussion.
13. Stessens, G.: *Money Laundering a New International Law Enforcement Model*. Cambridge, Cambridge University Press, 2000, pp. 211-12.
14. Passas, N.: *Informal Value Transfer Systems and Criminal Organizations*. The Hague: Dutch Ministry of Research and Documentation Center, 1999.
15. Shelley and Picarelli.
16. Shelley, L. I.: Crime and Corruption in the Digital Age. *Journal of International Affairs*, Spring 1998, 51, no. 2, pp. 607-620.
17. Passas.
18. Grabosky, P.: *Controlling Telecommunications and Cyberspace Illegalities*. New Brunswick, New Jersey, Transaction, 1998.
19. Some important thinking in this area is David Wall ed. *Crime and the Internet*. London and New York, Routledge, 2001; Grabosky, P.: *Unlawful Acquisition in Cyberspace*. Cambridge UK, Cambridge University Press, 2001.