Chapter XVIII
The Analysis of Money Laundering Techniques

Krzysztof Woda
European University Viadrina, Germany

ABSTRACT

There exist many connections between money laundering and terrorism financing concerning illicit practices for fundraising, transfer or withdrawal of funds. The characteristic multistage process of money laundering is also typical for the terrorism financing and often contains a series of transactions in order to conceal the origin or disposition of money. The purpose of this article is the analysis of the best suited techniques of money laundering for terrorism financing using electronic payment systems (like transfers, mobile payment systems or virtual gold currencies). Furthermore, the suitability of payment systems for conducting secret transactions for terrorism financing will be analyzed regarding the realization of a single phase of money laundering.

INTRODUCTION

Cyber terrorism is often defined as an attack against information systems, computer systems, and data, or, more generally, as disruption of critical infrastructures caused by information systems (Krasavin, 2000, as cited in *'Cyber terrorism' testimony*, 2000; Nisbet, 2003, as cited in Center for International Security and Co-operation). The definition of cyber terrorism can be limited to supporting activities for the purpose of preparing of terrorist acts (Krasavin, 2000). Such a narrow definition of cyber terrorism has many common characteristics with modern practices of money laundering (e.g., techniques for money transfers or disposition of money), which are mostly carried out by cyber systems.

The qualities of Internet communication, like anonymity, person-to-person payments, low communication and transaction cost, free transferability of assets between privates and banks internationally, and so forth, predispose the Internet for many illicit actions, like money laundering or fundraising for

terrorism. Some techniques of money laundering used to conceal or disguise the origin, nature, source, location, disposition, or ownership of assets can be used to conduct terrorism financing.

There are many questions concerning connections between money laundering and terrorism financing. For example, what are the most suitable money laundering practices operated through telecommunication networks, electronic banks (e.g., offshore banks) or with electronic payment systems that could finance terrorism (fundraising, transfer and withdrawal of funds)? Are the traditional money laundering techniques, as with shell companies and nominees, through unofficial money transfer systems, structured payments, wire transfers, and so forth, useful for financing terrorism or preparing for terrorist acts (Financial Action Task Force on Money Laundering (FATF), 2005)? How do the money laundering techniques differ with regard to their suitability for a single money laundering phase (and, thereby, for financing terrorism)?

CYBER TERRORISM AND MONEY LAUNDERING: DEFINITIONS, DIFFERENTIATIONS, AND CONNECTIONS

The broad definition of cyber terrorism is any kind of computer attacks against critical infrastructures, which does not differ from the definition of computer crime. Hence, many authors tried to concretize the definition of cyber terrorism (Krasavin, 2000; Nisbet, 2003; Pollitt, 1997). Pollitt (1997) combines the definitions of cyberspace and terrorism obtaining the definition for cyber terrorism. As a result, he defines cyber terrorism as follows: "Cyber terrorism is the premeditated, politically motivated attack against information, computer systems, computer programs, and data which result in violence against non-combatant targets by sub national groups or clandestine agents" (Pollitt, 1997, p. 2).

Nevertheless, this definition also contains areas or activities in common with computer crime (e.g., hacking) and, therefore, positions computer terrorism as a part of computer crime. Krasavin (2000, p. 2) defines computer terrorism as "use of information technology and means by terrorist groups and agents" and notes the motivation as a differentiation criterion from computer crime. The motivation of cyber terrorists is the use of computer systems and networks for the organization and execution of attacks; computer crime aims for the destruction of programs, infrastructures, or data (Krasavin, 2000). Institutions like the Center for International Security and Co-operation define computer terrorism narrowly as an attack against cyber systems (Nisbet, 2003, as cited in Center for International Security and Co-operation).

Money laundering is defined as an intentional committed offense that contains the conversion and transfer of properties of illicit origin (European Parliament and of the Council, 2001; U.S. Patriot Act, 2001). The purpose of money laundering is to conceal or to disguise the true origin, the nature, the disposition, or the controlling rights of properties that were acquired illegally (European Parliament and of the Council, 2001). Many assets are suited as potential properties for money laundering, such as cash, deposits, checks, and electronic currencies (e.g., prepaid payment instruments and virtual gold currencies), financial products, real estate, and services (e.g., in restaurants, casinos, or fictitious transactions in electronic commerce (e-commerce)). Operations like exchange, transfer, transport, acquisition, possession, or use of the properties for the purposes of the illicit money flows are typical of money laundering (European Parliament and of the Council, 2001;) U.S. Patriot, 2001). The new definition proposed by the Commission of the European Communities (2003) extends the present definition to terrorist financing (Article 1 of the Proposal for a Directive of the European Parliament and the Council, 2003, analogy in U.S. PATRIOT Act of 2001—Section 981 a(1)(G)).

Now supporting on the definitions of Krasavin (2000) and the Center for International Security and Co-operation, the connections between terrorism financing and money laundering will be searched. Krasavin (2000) refers to the preparing of terrorist acts (planning, logistics, and acquisition of objects