

3

Cybercrime and Cybersecurity in the Former Soviet Union and Central and Eastern Europe

3.1. Introduction

Many of the economies in the Former Soviet Union and Central and Eastern Europe (FSU&CEE) have become top cybercrime hotspots. According to Merchant Risk Council, half of the top ten economies from which most online frauds originated in the early 2000s were from this region: former Yugoslavia, Romania, Bulgaria, Ukraine and Lithuania (Sullivan, 2004). An estimate suggested that, in 2004, there were over 50 gangs of professional cybercriminals operating in Russia and Eastern European countries (Goldman, 2004). Organized crime groups in the region have reportedly developed expertise and are increasingly involved in cybercrimes (Giannangeli, 2008).

Cybercrime rings in these economies have mastered complex tricks and have increased pervasiveness and sophistication of cyberfrauds. Sophisticated frauds such as cyberextortion, distributed denial-of-service (DDoS) attacks and hijacking users' searches and clicks involve a complex fusion of strategy, technology, processes and people. Corruption, the lack of sufficiently high penalties, ineffective, inefficient, inadequate and weak legislation and lax law enforcement have fuelled cybercrime (Kshetri, 2005a). Likewise, key private sector players have indirectly encouraged cybercrimes. For instance, ISPs in the region arguably have no vested interest in fighting spam consisting of ads and malware as doing so would lead to a decrease in their traffic and hence revenue (Onyshkiv and Bondarev, 2012). According to the anti-spam organization Spamhaus, the Russian domain name registrar NAUNET allegedly harboured cybercriminals (<http://www.spamhaus.org/news/article/680/>). Despite the West's achievement to date in the battle

against sophisticated cybercrime, formidable challenges remain to fight cybercrimes originating from the region.

3.2. Assessing the nature, extent and impact of cybercrimes associated with the region

Cybercrimes originating in the FSU&CEE economies share two important characteristics. First, they are linked with organized crimes (Fitzgerald, 2008), which is clearly evident from many large-scale entrepreneurial initiatives (see Cases 1–3 and Table 3.1). Cybercrime groups in the region are well known for their efficient global teams and supply chain management, best adaptive global strategies, effective incentive structures and meaningful global collaborations (Goodman, 2011). For instance, IT security analysts observed that it required a large number of people to run the Rustock botnet (Table 3.1; bbc.co.uk, 2011d). The scales of activities needed to achieve the business goals create the need for an effective organizational design and execution (Sinuraja, 1995). More broadly, most economic and financial crimes in Russia and other former Soviet Union economies are associated with organized crime groups (Kuznetsova, 1994).

Second, unlike their counterparts in the rest of the world, cybercriminals based in these economies tend to pursue business models that offer quick monetization of their criminal activities. They prefer to steal financial information because it is more easily converted into cash than other digital assets such as trade secrets (Williams, 2011). To further strengthen this claim, it would be useful to consider cyberoffences involving the creation of fake profiles on social networking sites. In India and Arab economies one of the most popular categories of cybercrimes involves fake social networking profiles with the motivation to defame and malign the victim. Such offences in the former Soviet economies have a monetization aspect. In Armenia, for instance, criminals reportedly open accounts on social networking websites with the names of different people and use them to distribute pornographic contents. They then extort money to eliminate such pages by using threats (news.am, 2011). This is in sharp contrast to the approaches followed by cyberoffenders in other economies such as India and the Middle East.

We briefly discuss the situation in two internationally known cybercrime hotspots: Russia and Ukraine. Hackers from these countries have achieved a pace of innovation that is unmatched in the rest of the world.