December 2006

Toward an Adaptive Structuration Model of International Cyber-Crime

Kathleen Hartzel
Duquesne University

William Spangler
Duquesne University

Mark Grantz
United States Secret Service

Dennis Galletta
University of Pittsburgh

Toward an Adaptive Structuration Model of International Cyber-Crime

Kathleen S. Hartzel
Duquesne University
hartzel@duq.edu

William E. Spangler
Duquesne University
spangler@duq.edu

Mark Grantz
United States Secret Service

Dennis F. Galletta
University of Pittsburgh
galletta@katz.pitt.edu

ABSTRACT

Our research-in-progress uses Adaptive Structuration Theory to explain the evolving characteristics of cyber-crime – specifically, the increasing use of computing and networking technology by criminals to facilitate financial fraud and theft. Our goal is to understand the processes by which the perpetrators of cyber-crime form technology-based social networks.

Keywords

Adaptive Structuration Theory, appropriation, cyber-crime.

INTRODUCTION

This study explores the use of Adaptive Structuration Theory (AST) as a basis for explaining the evolving characteristics of cyber-crime – specifically, the increasing use of computing and networking technology to facilitate financial fraud and theft. In the context of our research, cyber-crime involves individuals from various nations, who are illegally exchanging money, merchandise and information within a collaborative computer-based social network. Our goal is to understand the processes by which the perpetrators of cyber-crime form technology-based social networks to respond and adapt 1) to technological change, and 2) to the changing tactics of law enforcement officials. In so doing, we ultimately seek to provide insights for business and regulatory decision makers, as well as recommendations regarding the types of strategies that might be effective in confronting this type of cyber-crime.

ILLUSTRATIVE CASES IN RE-SHIPPING

In order to provide a context for our analysis, we present two cases of cyber-crime involving re-shipping. These cases describe typical social networks involving cyber-criminal activity and the groups involved, as well as the processes and response strategies of both perpetrators and law enforcement. Re-shipping involves technologically-skilled individuals, often distributed internationally, who form social networks tied together through the internet. Essentially, the objective of these groups is to steal credit card numbers or bank account information, order merchandise for delivery to temporary addresses in the US, and re-ship the merchandise to middlemen. The middlemen in turn sell the merchandise and send the proceeds electronically back to participants in the criminal network.

The first case involves an investigation in Pennsylvania, which began with a tip from a local United Parcel Service (UPS) driver to the State Police. The driver noticed a sudden flood of merchandise being shipped to different addressees in the same apartment. After some investigation the state police arrested two Belarus natives. The state police charged them with receiving stolen property, but soon recognized the international nature of the crime and subsequently offered the case to the United States Secret Service (USSS). Prior to their arrest, one of the suspects' Belarus contacts had provided him with false identification, after which he began cashing stolen checks and reshipping merchandise overseas. In an attempt to stay ahead of law enforcement, the suspect would move from city to city every few weeks, but was ultimately unsuccessful.

The second case involves an American man recruited to do reshipping through an online game chat room. He agreed, but subsequently reconsidered his involvement and contacted the Pittsburgh USSS office. The USSS in turn directed him to contact the suspect and change the re-shipping address to a USSS-controlled location. The USSS corresponded with the

suspect via email and instant messaging, discovered that he was from Eastern Europe, and learned that the merchandise sent to them was to be re-shipped to a business in the western U.S.

During these transfers the USSS was able to capture an IP address that matched the country where they had believed the suspect was located. They also executed search warrants on his U.S. based email provider which provided further information about his operation. From the emails they learned that the suspect was being paid by a third-party company through a legitimate bank, from which they were able to discover account numbers and amounts transferred. They learned that the recipient bank was headquartered in Germany, and started the process of freezing the accounts. Legally, the U.S. can freeze assets from another country's bank without its consent, but this can be politically problematic and is usually not done without approval from senior officials in the U.S. government.

In this regard, the participation of foreign governments and law enforcement introduces additional stakeholders with goals and objectives that are potentially in opposition to those of U.S. law enforcement. In this case, the jurisdictional issues can become problematic. For example, in this re-shipping case, the suspect's home country had a history of not cooperating with U.S. law enforcement, which in turn contributes to the social structure of the criminal enterprise. Criminals in these types of countries will sometimes become complacent, believing that even if the U.S. knows who and where they are, their homeland will protect them. Surprisingly, this did not happen in this case. USSS agents were able to contact their counterparts in the suspect's country. They were told that the country in question does not extradite for this type of crime, but that they would prosecute in their own country – if a case could be built. Notably, as they were discussing the case, their counterparts in the suspect's country were able identify the suspect and confirm the information gained by the USSS. Increased information sharing of this type among inter-governmental law enforcement and the financial community tends to help control fraud, such as reshipping schemes (Swartz, 2005).

THE SOCIAL STRUCTURE OF CYBER-CRIMINAL ORGANIZATIONS

The cases presented above describe a problematic social structure in internet-based crime. Eastern European crime groups rely solely on the internet, along with the forums where an international open market for recruiting and directing participants is established. To succeed in an eastern European crime organization, one simply must be a reliable service or merchandise provider. Anyone, including law enforcement, can access these forums to buy credit card numbers and/or pay someone to send out spam email. Anonymity and protected identities are the norm. Because participants tend not to be within geographic proximity of each other, they generally do not meet their collaborators face-to-face, nor do they know their real names. Participants tend to communicate only through fabricated screen names, or 'nics'.

Victims in turn also are physically separated from individual criminal participants. While criminals are often based in Eastern Europe, victims tend to be corporations and individuals in wealthy western nations – particularly in North America and Western Europe. Consequently, the criminal and the victim – like the collaborators within the criminal organization – almost never meet face-to-face and rarely know each other.

The anonymous, virtual nature of this criminal organization poses a significant problem for law enforcement (Naim, 2005). In 'traditional' organized crime, law enforcement deals with names and aliases, and criminal transactions eventually require a face-to-face encounter. People generally know their counterparts even if they didn't deal with them personally. In this environment, the standard approach has been to arrest someone at the bottom of the criminal enterprise, 'flip' him, and then have him identify and provide information against the person to whom he answers. Law enforcement would work this 'ladder' approach in hopes of getting to the top. By contrast, in cyber-crime, people often do not know for whom they are working for and do not want to know.

In this environment, law enforcement has access only to a nic (which can be changed), an IP address (which can be masked), and a payment method. IP addresses are difficult to trace because there are many free proxy services that will route internet traffic through an intermediary computer. This means that if law enforcement is fortunate enough to obtain an IP address, it frequently identifies someone else's computer. Furthermore, internet service providers (ISP) tend not to retain IP addresses for an extended period of time, and even if they do, the information can be difficult to obtain. It is not unusual for an ISP in the U.S. to discard records more than two weeks old. European ISP's tend to retain their records much longer, but it is much more difficult for law enforcement agencies to obtain them due to different legal standards, language barriers, and so on. As noted, issues involving multiple jurisdictions can complicate investigations.

Payment methods also do not provide the solid leads they once did. The current preferred method of payment is through online companies that offer universal 'e-currency' backed (usually) by gold. Because these companies are generally located in countries other than the U.S., and because they do not use any nationally-recognized currency, they can avoid the regulatory requirements imposed on a standard bank. For example, the USSS is currently investigating a suspect having an

account with Webmoney, based in Eastern Europe. The USSS described sending money to the target's account as "like dropping cash into a black hole". Furthermore, because the company was not a bank and was not based in the U.S., they would simply ignore any subpoenas originating from the USSS. This allowed the suspect to withdraw his funds, perhaps funnel them through another internet money system, and then withdraw the funds and deposit them into his personal account – fully laundered.[1]

ELEMENTS OF ADAPTIVE STRUCTURATION IN INTERNATIONAL CYBER-CRIME

Adaptive Structuration Theory was first proposed by DeSanctis and Poole to explain how the social structure of an organization evolves through the interaction of groups with computer and networking technologies. (DeSanctis and Poole, 1994) A key aspect of these technologies is that they not only provide a basis for automating business tasks, but they also facilitate interpersonal coordination and information exchange – thus providing the potential for supplementing, changing or even subsuming the existing social environment of an organization.

The development of AST was motivated in part by a desire to explain the inconsistent performance of early group decision support systems (GDSS) (Gopal, *et. al.*, 1992-1993). While many of those systems were successful, many others were not. It was noted that different groups would use the same technology differently, even when addressing the same task. This suggested that group behavior was influenced and constrained, but not determined, by a GDSS. Conversely, the output of the GDSS was dependent on the development of a social structure engendered by the complex interaction of users, their tasks, the encompassing organization, and the technology.

We posit that appropriation of internet technologies by international cyber-criminals is explainable by the same theoretical constructs used to model the social impact of GDSS. Specifically, the fraud case described above exemplifies, within the context of AST, how social structures evolve and adapt to the interactions of the various stakeholders. Essentially, the evolution of social structures occurs because of three characteristics of today's technology. The first is the availability of the internet – i.e., a distributed, world-wide communication network. The second is the transition from a need for face-to-face communication to one based more on virtual communication. Virtual communication refers to the capability of groups to organize in an anonymous, on-line forum, where their physical characteristics and actual identity are unknown. The third characteristic is the change from relatively persistent relationships among participants in the criminal network, to relationships that are more transient and transactional. Face-to-face relationships create member vulnerabilities, given the potential for associates to trade information about identities in exchange for favorable treatment by law enforcement. Thus, in the traditional criminal organization, participants are motivated to limit the number of individuals involved, which leads to smaller groups and longer-term relationships. Conversely, the anonymity of virtual organizations mitigates the risk of exposure by others. Thus, membership in the organization tends to be more open, and individual involvement tends to be based primarily on transactions rather than relationships.

Table 1 summarizes the issues discussed in the cases above. It describes the structuration of the social network as it transitions from a traditional financial fraud and theft organization to an international cyber-crime organization, and suggests how the network changes through group appropriation of internet technologies.

AGENDA FOR FUTURE RESEARCH

This research focuses on the growing international nature of financial fraud, and the increased ease with which criminals are able to access and transfer stolen financial information and money. This research seeks to develop a theoretical framework through which the changes in cyber-criminal tactics engendered by the rise of the internet can be explained and predicted. We intend to use Adaptive Structuration Theory as the basis for future study. Although AST was developed to explain GDSS effectiveness, where the systems are primarily commercial and proprietary, we believe that elements of the theory are generalizable to criminal groups who are using the Internet to collaborate. Specifically, we will consider how the availability of the Internet has allowed those involved in financial fraud to appropriate technology in new and changing ways. We will also consider how the composition and norms of criminal alliances are evolving in response to emerging technological features. Finally, we will explore how law enforcement can use both the internet and traditional measures as countermeasures in the war against international cyber-crime.

---

[1] . We should note that Webmoney was eventually shut down by its host country as a result of pressure from the E.U. and other Western nations.

Table 1: Structuration Elements in the Internet-based Social Network

	Traditional	Internet-Based
Group Composition	• Members of the criminal organization are known by – and physically recognizable to – other participants in the organization • Membership is relatively stable given the risk of conspirators "flipping", or betraying their associates	• Members can be known only through aliases, and are not physically recognizable to other participants • Membership can be more volatile or fluid given that the actual identity of a participant can be masked
Group Proximity	• Members tend to be located in the same geographic region. Although telephone, fax, and mail communicate alleviate the need for face-to-face communication, they do not facilitate the efficient exchange of misdirected financial information	• Members can be more easily distributed. This facilitates the formation of international cyber crime networks that can take advantage of the bureaucracy and politics that hinder the efficacy of law enforcement response
Victim Proximity	• Victims tend to be located in the same geographic region as the criminal. If the crime is computer-base, access to the physical machine is required. If the crime is socially-engineered, victims will recognize foreign accents and remote mailing addresses	• Victim proximity tends to be based upon factors that include the difficulty of catching the perpetrator, affluence of the victim, lack of technical security, and lack of extradition agreements. These factors tend to correlate with the physical distance between victims and criminals.
Jurisdiction	• Given the close proximity of criminal group members and victims, the number of jurisdictions involved in prosecutions tends to be smaller	• Given the physical distance separating group members and victims, the number of jurisdictions involved in prosecutions tends to be larger
Payment Methods and Characteristics	• Hard currency • Electronic fund transfer	• E-currency • Payments for goods delivered • Payments for non-delivery

REFERENCES

1. DeSanctis, G. and Poole, M.S. (1994). Capturing the complexity in advanced technology use: Adaptive Structuration Theory, *Organizational Science*, 5, 2, 121-147.
2. Gopal. A., R.P. Bostrom, R. P. and Chin, W. (1992-1993). Applying Adaptive Structuration Theory to Investigate the Process of Group Support Systems Use, *Journal of Management Information Systems*, 9, 3, 45-69.
3. Niam, M. (Oct. 24, 2005). Broken Borders – Trafficking: Globalization has lowered barriers to illegal as well as legal commerce, and international smuggling now threatens to derail the world economy. *http://www.msnbc.msn.com /id/9711920/site/newsweek/from/RL.2/*
4. Spencer, S. (2/18/2005). Secret Service: Internet fraud threatens U.S. economy. *http://www.usatoday.com /tech/news/computersecurity/infotheft/ 2005-02-18-fraud-threat_x.htm*