See discussions, stats, and author profiles for this publication at: <https://www.researchgate.net/publication/280204406>

A Conceptual Review and Exploratory Evaluation of the Motivations for Cybercrime

Research · July 2015

DOI: 10.13140/RG.2.1.4358.5129

CITATIONS

0

READS

431

Some of the authors of this publication are also working on these related projects:

Cyberwarfare [View project](#)

**A CONCEPTUAL REVIEW AND EXPLORATORY EVALUATION OF THE
MOTIVATIONS FOR CYBERCRIME**

Troy Emilio Smith

16/08/2013

A CONCEPTUAL REVIEW AND EXPLORATORY EVALUATION OF THE MOTIVATIONS FOR CYBERCRIME

INTRODUCTION

Technology and the Internet play pivotal roles in all aspects of society - business, finance, politics and communication. The migration of society to the digital age has seemingly come with the movement of conventional attacks to the cyber-world¹. Terrorists, criminals, cartels, activists and cultural extremists all employ cyber-attacks². This trend is facilitated by the advantages the cyber-world offers to would be attackers; one such is the asymmetric nature of attacks. The Internet can be considered asymmetric in terms of comparative effort to degree of damage and in also attacker to victim ratios. Global information communication technology [ICT] may be manipulated for committing criminal acts, with transnational reach³. Additionally, the cyberworld poses unique challenges for law enforcement, namely; anonymity that is intrinsic to the cyberworld, flexible identities and the ineffectiveness of local and international laws against cybercrime. The ineffectiveness of laws is particularly important, as cybercrime tends to have no specific geospatial identity; it operates globally with access only limited by the reach of the Internet itself⁴. Therefore, cybercriminals can exploit different legal frameworks adopted by various nations, so that even if attribution were not a problem, prosecution of cybercrimes relative to conventional crime would be very small. These advantages are important to note, as they will form the foundation for research into the motivations for choosing cybercrime over conventional crime to achieve a target/goal. The motivation according to the parameters of this research relates to the drivers that propel the

person to commit a cybercrime rather than the rationale in choosing to use cybercrime as opposed to conventional crime. Of particular importance is the anonymity associated with the Internet, which can act as an enabler to persons encouraging them to commit acts of crime or aggressions in the virtual world that they would never commit in the physical world.

Cybercrimes refer to offenses in the digital realm (virtual environments, networks etc) as well as use of the Internet to commit crimes. In July 2012, Keith Alexander head of the National Security Agency and U.S. cyber-command said cyber-attacks increased by forty-four (44%) percent in 2011 and now account for the "greatest transfer of wealth in history." The 2012 Cost of Cybercrime Study discovered that cybercrime was costing some companies over 8.9 million U.S. dollars per year⁵, as attacks resulted in loss of intellectual property, goods, services, money, operation time and the need for system repairs. In addition to direct financial damage, businesses must also consider indirect cost due to loss in sales, loss of confidence by current and potential customers, staff time and other resources that must be used to fix the damage left by attacks and to implement new security measures. Given the increase in cyber-attacks and the large financial loss associated with it, cybercrime is of primary concern to law enforcement. As such, there is ongoing research to develop measures to prevent, mitigate and investigate cyber-attacks.

Traditionally research has focused on the digital side of cyber-attacks; this is the technologies used and how they interact with networks and computing infrastructures. However in 2010, a former Defense Department official said, "agencies responding to real-time coordinated cyber-attacks must focus not only on eliminating the immediate threat, but identifying the attackers' motives"⁶. Combating

cybercrime calls for a focus on the very foundation of conflict and crime, which is motivation. Computer crime is an intentional act requiring organization and thought, therefore, there must be suitable motivation for a person to engage in this type of crime given the possible consequences. In order to model cybercrime as a conventional crime, a socio-technical perspective is applied and examined in order to understand cybercrimes and categorize them. The analysis of motivations for cyber-attacks will give insight into modus operandi of cybercriminals.

Understanding motivation is a pivotal step in law enforcement efforts as it is integral in profiling the attacker [goal, method, victim and capability]. The distinction between cybercrime and other cyber-based malicious acts is motivation. Without understanding the motivation or criminal intent, cyber criminals and other malicious actors may appear to be similar, causing confusion when legislators or the judiciary seek to categorize an activity as a cybercrime. All these factors support the importance of criminal profiling in crime prevention and suppression. Related, specific acts can be organized into groups making it easier to collect relevant statistics and allow law enforcement agencies to convene special units to target specific categories of crime. More importantly motive is an important element in proving guilt in any Justice system. In any criminal case the court must demonstrate means, motive and opportunity. Thus, understanding the criminal's motive is important at two distinct phases of criminal investigation; when creating a profile to identify the suspect and when the case is being presented to the court. Understanding motives is also essential in planning and policy development as it helps to identify potential victims and their vulnerabilities. Planners and policymakers can use this information to

develop strategies to educate specific groups and to create awareness among would-be victims.

While a number of crime theories may be applicable to help elucidate the nature of cybercrime, the fact that cybercrime represents a new and distinct crime perpetrated within the unique medium of cyberspace, creates challenges to the direct use of general crime theories on both psychological and spatial levels. Within cyberspace, persons may demonstrate extreme changes in their level of conformity as compared to the physical world as they feel empowered by the anonymity the cyberworld offers. Additionally, variables such as flexible identity and lack of deterrence factors provide incentives for criminal behavior in cyberspace. Therefore, before seeking to superimpose conventional theories onto cybercrime an initial phase of research based on case analysis and observation should be performed.

This paper will identify cybercrimes into four (4) broad categories of motivation. These build upon the Federal Bureau of Investigation's three primary categories of cyber threat actors; organized crime groups, state sponsors and terrorists groups. The "organized crime" category focuses on those motivated by financial gain, while the "state sponsors" category deals with the use of cyber attacks to fulfill some political or international relations agenda. The Congressional Research Service states that the third category of actors is motivated by ideologies⁷. This provides three categories for the motivation for cybercrime, namely; economics, politics and ideology. However, another motivation must be added, which is not accounted for in the FBI analysis to account for hackers, stalkers and online child predators. These individuals are uniquely motivated by emotional/behavioral impulses. The identified categorizes have been further subdivided to help

demonstrate how they act as motivations which express themselves in the resultant criminal acts. Once the categories are established the relationship of motivation to the wider profile will be demonstrated in a tabular format. This will serve to demonstrate that motivation can be used to categorize cybercrime and to provide an alternative to the traditional method of using technology generated categories to understand cybercriminals. The four (4) broad categories of motivation to be utilized in this research are ideological, political, economic and behavioral/emotional.

LITERATURE REVIEW

A wealth of academic literature exists on the use and nature of cyber-attacks as a result of its role in social dissidence and warfare. However, there has not been a strong focus on motivation for cyber-attacks or intricate profiling of attackers. Generally, if motivation is considered it is localized to a specific type of attack. Categorization tends to focus on the digital side rather than on the human aspect for the use of cyber-attacks. The greatest attention to categorization of cyber-attacks has been localized to cyber-crime. It should be noted though that in some publications, the term cybercrime has been stretched to encompass cyber-terrorism and espionage. As the use of cyber-attacks has become more prevalent there has been a paradigm shift to increase focus on methods to prevent cyber-attacks, which focus on the attacker rather than the methodology. Recently, cyber-security experts and scholars have highlighted a shortcoming in research into the motivations for cyber-attacks. Also the current inadequate profiling of cyber-attackers may be one key hindrance in the effectiveness of law enforcement's apprehension of cyber-criminals. As such, there is a paucity of scholarly information on the motivations for cyber-attacks.

Ngafeeson using motivational theories found that business studies proposed one of the few motivation-based models for cybercrime classification. She writes that with cybercrime like conventional crime there is a need to understand three factors: identification, classification and the implementation of effective counter-measures (Ngafeeson 2010). Ngafeeson deems motivation to be the very foundation of crime itself, and that crime whether cyber or conventional share the same motivations.

Roy expressed similar views to Ngafeeson in regards to the relationship between cybercrime and traditional crime. He believes that there is no distinction between cyber and conventional crime as both crimes result in some loss to one of the parties; the only real difference is the medium (Roy 2008). Liu who suggested that the motivation for specific areas of cyber-attacks such as cyber-crime remained the same as in conventional crime further supported this overlap of cyber and conventional crime. The shift/ increase in cybercrime is due to increasing awareness of criminals and crime groups to the benefits of crime in the cyber-sphere vs. conventional crime.

Cross identifies the following as the main reasons for committing cybercrime: financial, emotional, intellectual, curiosity, deviant behavior and to acquire access to restricted or copyrighted material (Cross 2008). This generally overlaps with other literature written that references motivation for cybercrime.

Shinder believes that profiling is an essential tool for law enforcement, and in the case of cyber-attackers is based on five characteristics; level of technical knowledge, level of disregard for the law/ ability to rationalize an unlawful act, tolerance to risk /need for thrill and motive (Shinder 2010). Motive being a key factor in narrowing the profile and potentially making a case against an attacker. The possible motives for cybercrime that were highlighted are money, emotion, sexual impulses, politics/religion and fun.

Even though the availability of scholarly literature is limited on categorizing cybercrime by motivation, there is wealth of information on the discrete areas of cybercrime; motivation theories and profiling that can be mirrored to this research. The Literature provides a basis to determine what is the consensus by academics and

professionals towards motivations as a factor in committing cybercrimes. This initial analysis of the applicability and usefulness of a motivation-based model for classification will encourage additional research to determine which aspects are truly applicable.

ANALYSIS

Although technology is the tool and cyber-sphere the medium, we cannot forget that cybercriminals are people. Therefore, one way of analyzing cybercrimes is to interpret them as digital versions of conventional, real world offenses i.e. they can be considered to be conventional crimes that incorporate a virtual or cyberelement⁸. People commit crime when contributing factors cause them to become motivated to carry out criminal behavior. Without motivation, even if opportunity and vulnerabilities are present according to the Routine Activity theory¹ a crime will not occur.

The following is an analysis of the individual motivation categories identified in this research of cybercrimes and cybercriminals. In this paper motivation refers to the factors that “push” individuals to commit cybercrime. These motives are as a result of the determinants of crime, for example; unemployment, low income, poverty, wage inequality, social status, oppression, sexual depravity etc⁹. There is an innate desire to overcome these determinants in order to fulfill or satisfy “needs” such as economic success, sexual gratification and freedoms of speak. This desire

---

¹Rational choice theory is based on the fundamental tenets of classical criminology, which hold that people freely choose their behavior and are motivated by the avoidance of negative stimuli and the pursuit of positive stimuli.

motivates individuals to commit crime and can be used in many cases as justification for their actions. The identification of the main and sub-categories are the result of a review of the literature and case analysis.

Due to the dynamic nature of the human psyche any action is generally governed by multiple motives, however, to facilitate categorization in this paper, focus will be placed on the dominant motive for each group identified.

While the basis of the categorization is motivation, the end goal is a contribution towards profiling cybercrimes, which consists of numerous variables. Table 1 shows some of the main variables, which affect the motivation behind committing the crime. This table helps to demonstrate the important role that motivation plays in crime and its relation to identifiable elements, which can be examined to build a profile on suspect(s). Therefore, through examples and analysis, other variables will be introduced as they relate to the four (4) categories.

Table 1. Main variables affected by the motivation of the person engaging in cybercrime

VARIABLES	DEFINITIONS	SOME KEY QUESTION ASKED
Selection of Victim	The cyber-criminal chooses a target (individual, private organization, government entity) based on given criteria/motive	Was the victim an individual, organization, political group or nation state? What attracted the attacker to this particular victim? Was the victim lured? Does the attacker seem to know the victim personally?
Nature of Attack	The cyber-criminal depending on his goals and motivation has different modus operandi. For example he can choose whether stealth is necessary or if he can launch the attack by himself or is a group attack needed.	Covert vs. Overt? Did attacker claim responsibility? Where threats made before attack? What was the location or degree of spread of the attack. Could it be identified as a one to one, one to many or many to one attack?
Goals	The purpose of the attack. What did the attacker hope to achieve, by using a particular type of cyber-weapon.	Money stolen vs. Information stolen vs. Disruption vs. Serious Damage What need/desire did the attack fulfil? Was there financial gain by the attacker?
Technical Resources	The level of skills the attacker has and the type of cyber-weapons he uses.	How sophisticated was the attack? Skill of the attacker Complexity and efficiency of cyber-weapon used? How strong was the security Barrier?

IDEOLOGY

Some cybercriminals are motivated by ideal(s) or belief(s) they hold dear. These ideals or beliefs can come from religion or a societal construct. They tend to use a strong-arm approach through attacks to coerce people and governments into supporting their ideology. In this paper ideology is subdivided into religion and causes in order to analyze the two main groups motivated by ideology, which are cyber-terrorists and “hacktivists”.

Religion

Cyber-terrorism can be defined as unlawful attacks and threats against systems, networks and electronic information to create fear, chaos with the goal of intimidating or coercing a government or people in furtherance of ideological objectives¹⁰. Cyber-terrorists are motivated by radicalized religious beliefs and use their interpretation of religion as justification for their actions and can escalate to compel persons not normally associated with violent behavior to elevated levels of deviant behaviour. These terrorists are well funded and have developed a wide range of skills that can prove formidable to cyber-security systems. This is the result of opportunistic collaboration with nation-states and criminal ventures¹¹.

Terrorists much like other criminals have discovered the advantages of the cyber realm in furtherance of criminal ventures. The increased amalgamation of technology into critical infrastructure has made it a prime target for terrorists. Terrorists utilize the Internet to acquire and learn about weapons, launch cyber-attacks, spread propaganda and to recruit new members. However, this is not the only use of cyber-attacks by terrorist. Cyber-attacks are also used to gain finances that

can be used to purchase weapons and fund general terrorist activity. Terrorist will normally claim responsibility for their cyber-attacks, as anonymity in this case, would defeat the goal of creating fear and forcing coerce of governments. The attacks must cause, as much disruption as possible, and the victim must know that they are at the mercy of terrorists.

Terrorist groups such as Hezbollah are ranked high internationally for their ability to carry out cyber attacks¹². This shift to cyber-attacks by militant groups such as Hezbollah is due to ease of use, increased range and availability of targets, the asymmetric nature of cyber-attacks and anonymity when they use it for raising funds for terrorist activities. The asymmetric nature of the Internet and its range are especially enticing as terrorist can now affect a large number of systems/ create major disruption with limited human resources from relatively anywhere in the world. Hezbollah showed its increasing technological sophistication in 2006 when they launched over 10,000 cyber-attacks on Israel in retaliation to Israel's bombing of Hezbollah targets in Beirut¹³. In October 2008, The Islamic Egyptian Muslim Brotherhood movement published a fatwa declaring cyber-attacks against American and Israeli websites as allowed by Islamic law and an acceptable form of jihad¹⁴. According to the chief of the U.S. Cyber Command Al-Qaeda is also seeking the capability to launch cyber attacks against U.S. networks¹⁵.

While cyber-attacks by terrorist are of great concern they are not currently the major threat, as their ability to cause significant damage has not yet been realized. The greatest threat is the use of the Internet for recruitment through the spread of propaganda on their websites. Under United Nations Security Council resolution 1373, nation-states are required to suppress the recruitment of members of terrorist

groups through some form of legislation, in support of international anti-terrorism strategy¹⁶. In the United States this is covered under 18 USC § 2339B, which makes ‘material support’ of terrorist groups a criminal act punishable by imprisonment¹⁷.

In 2008, the Singapore government arrested Muhammad Zamri Bin Abdullah for his involvement in activities that posed a potential terrorist threat. Zamri was self-radicalized by radical propaganda on the Internet. Terrorists have found the Internet to be very useful in recruiting people who were generally neutral about terrorist causes. They use the Internet to portray themselves as victims that use violence as a last resort against aggressive oppressors. Such was the case with Zamri, who became so radicalized that he left his home in Singapore and attempted to join a ‘mujahidin network’, which he hoped would allow him to receive training so that he could wage armed jihad in Afghanistan¹⁸.

Cause

Hactivists are motivated by belief in a cause based on social or personal interests that can extend past their nation’s borders. They tend to take direct and aggressive actions against computers and computer networks to achieve a social goal. They use their skills, and the power of the Internet to battle causes such as hegemony, authoritarian rule, oppression and information ethics. If they believe an injustice is being done they will attack individuals, companies and even nation states¹⁹. The term hactivist when coined in 1998 was meant to symbolize the use of technology to advance human rights and freedom of information. Two of the most famous hactivist groups Anonymous and Lulzsec claim their actions support Article 19 of the United Nations Universal Declaration of Human Rights²⁰. This broad goal to advance

political or social agendas that do not necessarily relate to their country of residence/citizenship is the key difference between hacktivist and the closely related political resistance groups that utilize cyber-attacks.

Hactivism can be considered social mobilization for the technology age. Hacktivists tend to use web defacement and Denial of Service Attacks as their major weapons of choice. Denial of Service attacks can be considered virtual sit-ins, which serve to disrupt industry and civil practices or temporarily dismantle production and circulation of commodities within a state²¹. When hacktivists focus Denial of Service attacks at corporate operations, such as the electronic banking systems at public access points e.g. ATM and point-of-sale machines, they have the potential to systemically disrupt marketing and sale of commodities. They also put their talents to work by organizing piracy, DNS hijacking and replacing homepages with ideological messages²². They tend to make their attacks as public as possible and usually take credit for their actions. Their attacks are normally grand and short-lived as they aim to draw attention to their cause and not necessarily inflict long-term damage. They demonstrate their power as ‘watch dogs’ against injustice, willing to punish those they believe are being unjust.

The major concern for law enforcement is the increasing use of information theft by hacktivists. In 2011, hacktivist groups like Anonymous engaged in activities to spread democracy such as providing technology, skills and services to nascent democratic protestors in the Middle East. However, many other hacktivist groups focused on increasing attacks against Western government and economic institutions. Data thieves release information on 46, 000 members of an amnesty program for unpaid traffic tickets in Alabama along with the personal information of

law enforcement officers from Arizona. The results of a study by Verizon stated that 58 percent of the data thefts in 2011 were committed by hacktivists²³. This revelation has made cyber security professionals and law enforcement begin to consider hacktivists potential national security threats, since they appear to be an even greater threat to data security than organized crime groups and nation states combined.

POLITICAL

Political motivation for cybercrime can be viewed at two levels, the level of the state actor and at the level of the non-state actor. At the non-state actor level political motivations are closely related to emotions, as people can become very passionate about politics. Political motivation at this level is often associated with right wing groups. At the state actor level politics and foreign policy motivates countries to use sabotage and espionage to maintain political and/or military advantage. This category of motivation can best be explained by reviewing the two subcategories of political resistance and cyber-warfare/cyber-espionage.

Political Resistance

The Internet has altered the manner in which political discourse and advocacy take place, particular as it relates to affecting foreign policy. The Internet has given increased power to grass roots resistance through its asymmetric nature. Private citizens can now act on their own initiative against an enemy of the state, which they consider to be a threat²⁴. The political activists can be considered to be patriotic or nationalist hackers, who believe they are fighting a war for their country or the rights of a set group within the country. Unlike hacktivists who have a cosmopolitan agenda,

fighting for international right of freedom and other liberties, nationalist hackers have narrow nationalistic views. Hence, they tend to identify themselves in nationalistic terms such as Israeli, Palestinian and Iranian²⁵. They can be compared to classic right wing activist wanting to stifle opposition through a show of force. They are only concerned with nationalism and patriotism and are willing to inflict maximum damage against opposition to achieve their goals.

Cyber-resistance utilizes a growing botnet population to launch Distributed Denial of Service attacks, deface websites or leak data. These methods are used since they are cheap, widely available and call for relatively little technical skill, while serving to multiply the force of the attacker. The computers used in political cyber-attacks can be bots in a botnet army or a coordinated effort of numerous resistance members/supporters who willing install the necessary software on their computers. Distributed Denial of Service attacks cripple target networks by making them unusable, with the intent of inflicting damage or to silence opponents by making their resources inaccessible²⁶. The hacker groups used to launch these Distributed Denial of Service attacks lack permanent structure and membership, emerging temporarily when needed.

Cyber-attacks used for political resistance are less frequent than other types of attacks, as they are used to treat with a specific grievance. They are normally identified based on internal information, such as the nature of the victim and the attack commands seen. They are then validated by comparing them chronologically with reports of diplomatic grievances and intended redress via online attacks.

Cyber-warfare/Espionage

Cyber-warfare is the use of politically motivated cyber attacks on adversary networks or systems to conduct sabotage and espionage²⁷. Nation-states leverage offensive cyber-warfare with hostile intent hoping to disrupt or destroy systems of their adversaries. They can either utilize home grown hackers or hackers for hire to launch these attacks. Nation-state actors have an advantage over other types of cyber-attackers due to their larger budgets and availability of resources. They can dedicate time and personnel to cyber based efforts to produce highly skilled hackers with the best cyber weapons. The scale of effort, choice of victims and the technical sophistication of the cyber weapons are used to identify attacks sponsored by nation-states.

Cyber-warfare is a favorable option to nation-states as it allows them to attack other nations, sabotage systems and steal information with relatively no possibility of escalation to conventional warfare. No other resource can give a nation-state as much access to sensitive information with so little physical effort and low probability of attribution. In the cyber realm, offensive measures are facilitated by the priority given to information sharing and accessibility over security. In this new interconnected world using an enemy's integration and dependence on technology to spy and attack them from a computer in another continent is preferred to conventional warfare. Many of the same political objectives formally achieved through physical warfare and espionage can now be done without endangering the lives of citizens.

As stated in the definition for cyber warfare, nation-state cyber attacks focus on the two main goals; sabotage and espionage. Sabotage was the goal during the alleged attacks by the Democratic Republic of Korea on the United States and South Korean government websites in 2009. In both cases, Distributed Denial of Service

attacks were used to disrupt the functions of the government websites. While sabotage is common in cyber warfare, espionage is currently the predominant form of cyber warfare. China and Russia have been identified as leaders in this form of cyber warfare, with large departments dedicated to developing cyber-warfare tools. One of the notable espionage efforts of China is “Titan Rain”. Titan Rain is the collective term given to a series of ongoing attacks by China on the US Department of Defense since 2002. The Chief of War-fighting Integrations indicated that China had downloaded 10 to 20 terabytes of data from the Department of Defense’s Non-Classified IP Router Network (NIPR)²⁸. Cyber-warfare has become an increasing concern for national security officials as methods become more efficient and have increased in frequency.

FINANCIAL GAIN

This category includes anyone who uses cybercrime for financial gain. This can be a trusted insider, a corporation, a lone hacker or an organized crime group. These cyber-criminals utilize a variety of techniques within the cyber-sphere to facilitate their money-making efforts. These efforts can be either computer-based or computer-assisted. Some of their criminal endeavors utilize cyber attacks while others use social engineering to “con” people into releasing personal information or money. Cybercrime for financial gain can be subdivided into two categories, namely; corporate espionage and criminal enterprise.

Corporate Espionage

Throughout this section, corporate cyber espionage will be defined as the use of computers or related systems in targeted attacks by non-state actors, in order to

steal sensitive information or enable operations that sustain covert access to secure data held by private organizations. The non-state actors launching these attacks tend to be companies or financial firms²⁹. Companies seek to get a competitive edge by getting information on products and designs. Financial firms hope to obtain information on the activities on various companies to guide their market trading.

Targeted attacks use spear-phishing, social engineering, windows exploits, directory compromises and remote administration tools to gain unauthorized access to sensitive information³⁰. Victims are specifically targeted based on access, strength of security and/or susceptibility/naivety to social engineering techniques. In 2011, 29 companies in several sectors were targeted using emails disguised as meeting invitations from known suppliers. These emails contained a Trojan that could be used to steal sensitive information about plans and designs from the target companies.

Companies use targeted attacks as a tool for espionage in long-term cyber-assaults, normally targeting high-value information/systems in private and government agencies. In 2012, the number of targeted attacks was approximately 101 per day an increase of 24 percent from 2011 and a 32 percent increase from 2010³¹. Numerous cyber- espionage campaigns against the petroleum industry, NGOs and the chemical industry were discovered in 2011. One of these attacks was against a US defense contractor, which resulted in the loss of 24,000 files. The files contained sensitive information related to weapons system being developed for the Department of Defense (DoD).

Recently there has been a change in the modus operandi in corporate espionage i.e. a shift from attacking large organization to smaller companies. A 2013 Internet security threat report issued by Symantec indicated that businesses with

fewer than 250 employees are the fastest growing target of cyber-attacks. This change in targeting could be a result of larger organization using their substantial resources to increase security. In order to acquire the same information with the limited resources utilized by some of these corporate attackers, subcontractors with weaker security barriers are becoming the new targets.

Previous paragraphs focused on the attacker being a corporate entity; however, “insiders” are increasingly committing acts of espionage. Insiders can be current, former or temporary employees, software suppliers or service providers such as consultants and independent contractor. Insider threats can be triggered by professional dissatisfaction, the perception of being unjustly overlooked for a position or being dismissed. Being treated unfairly or the perception of being treated unfairly can lead to a desire for retribution, which they use as justification for criminal acts against the organizations. Insiders can be more problematic than corporate entities; although they do not have the resources and expertise as professional hackers they have intimate knowledge of systems, defense and access protocols. Instances of insider attacks tend to increase during times of recessions when jobs are being lost, persons are overworked and there is a general dissatisfaction among workers who eventually succumb to economic strains³². The insider may decide to steal information and/or intellectual property to sell a rival company or may have been recruited by another company. In 2010, Sergey Aleynikov a computer programmer for a Wall Street company was found guilty of theft of trade secrets. Aleynikov transferred 32 megabytes of the company’s intellectual assets and attempted to hide his activity. However he was discovered by the company’s routine network

monitoring systems. This is just one instance of a growing trend, in 2011 attacks by insiders accounted for 21 percent of attacks against businesses in the United States.

Criminal Enterprise

Criminals have discovered that technology has created many opportunities for illegally gaining wealth. Both individual criminals and organized crime groups utilize the Internet and computers in their criminal activity. There are essentially three ways criminals use the Internet in their criminal efforts. First, cyber-attacks are used to penetrate computers and networks to steal personal data and extort businesses with threats of attacks or exposure of sensitive data. Secondly, social engineering is utilized to trick computer and network users to divulging sensitive information. Thirdly, the Internet is used to facilitate illegal enterprises and enterprises that facilitate illegal activity. No matter the way the Internet is used the goal remains the same, to make money.

Financially motivated attackers are indiscriminate in their attacks; they generally throw a broad net of online scams and phishing expeditions in the hope of getting as many victims as possible. They use these scams and social engineering to steal identities, get banking information and to siphon money out of bank accounts. Identity theft complaints in the United States have moved from 1.4 million to 2 million an increase of 41 percent in the period 2010 to 2012. The Federal Trade Commission reported that identity theft incidents in 2012 were distributed as follows; Government documents/benefits fraud (46%), card fraud (13%), phone or utilities fraud (10%), and bank fraud (6%), employment-related fraud (5%) and fraud (2%)³³.

Victims of identity theft either had their credit accounts used fraudulently or their information used to open new credit accounts.

Organized crime groups in Eastern Europe and numerous other locations are increasingly using cyber-attacks on companies. They attack the companies and threaten to either launch disrupt/damage their operation or release stolen sensitive corporate data unless they are paid large sums of money. Their weapon of choice when issuing threats to companies is Denial of Service attacks.

Criminals also attempt to amass wealth by using/creating pornographic websites, online scams and online gambling websites. Two known cases of Internet crimes related to pornography are the Delhi BalBharati case and the Bombay case, where two Swiss couple would force slum children to appear in obscene photographs. These photographs would then be uploaded to pedophile websites³⁴.

University of Hamburg economist Ingo Fiedler in a report to the European Commission in 2012 said organized crime groups rely on online gambling sites to launder money³⁵. Online gambling sites are ideal for money laundering due to the large volume of transactions, the absence of a physical product, tax-free winnings, multiple payment methods and the anonymity possible for users and owners.

EMOTION

Emotion is one of the most unpredictable categories, as there is often no planning. These attackers use the Internet as a means of acquiring fame, getting revenge, expressing anger or to satisfy sexual impulses. The use of cyber-measures is often unplanned and in many cases consequences are not assessed. Generally, with the

exception of crimes motivated by the subcategory of sexual impulse, the attacker does not intend any major damage, although this sometimes results. To better analyze this category it has been subdivided into three (3) subcategories, namely; notoriety/challenge, revenge/anger and sexual impulses.

Notoriety/Challenge

Persons motivated by hopes of notoriety of just seeking a challenge tend to be teenagers and sometimes even younger individuals³⁶. They engage in network intrusions, theft of intellectual property and deface websites. They do not launch attacks with malice, although the victim who incurs the cost of their fun may have a different opinion. These hackers have often only wanted to prove that they can perform these cyber-attacks, to themselves and/or their peers.

Script Kiddies, is the derogative name given to hackers that use borrowed programs to attack networks and deface websites in an attempt to gain popularity. Since they act without a code of ethics like hacktivists, strict ideals or allegiances, they are very unpredictable. Choosing a target can be based on access, not wanting to pay for software, a dare or a bad experience on a website. However, similar to hacktivists, they will take credit for any attack they commit. It should be noted that they may become motivated by possible financial gain at any time and may sometimes be hired by independent parties.

In 2007, teenager George Hotz purchased an iPhone from AT&T; however, he wanted to use it on the T-Mobile network. Through research and connecting with hackers online he met the self-assigned challenge to unlock the iPhone. He achieved his goal by scrambling the code on the phone and then writing a

program to use the phone on any network. Proud of his achievement he broadcasted his work on YouTube to the delight of over two (2) million viewers³⁷. This is a common series of events for this category of hacker, who hack to achieve a personal goal/benefit and seek as much recognition as possible for their triumph. Hotz wanted an unlocked phone because he thought he had the right to use the phone he paid for as he liked, the potential millions of dollars lost to AT&T by other persons using his method probably never crossed his mind.

Revenge/Anger

Cyber-attacks can be used as an outlet for seeking revenge or expressing anger. The attackers may be spurned lovers or spouses/ex-spouses, disgruntled or fired employees, dissatisfied customers, feuding neighbors, students angry about a bad grade, to name a few. Even a loss during online gaming can cause someone to launch a cyber-attack³⁸. The ease of access to hacking toolkits is one of the major contributors to this phenomenon. Anyone can become a hacker overnight and have the ability to launch a cyber-attack on anyone they believe did them wrong with little effort or fear of being caught. These attackers steal personal information, hijack emails, deface websites or social media accounts and launch Denial of Service attacks. Their victims can be individuals or companies, even government organizations in some cases. Attacks against gaming sites and forums, where player-on-player attacks happen, seem to be predominantly motivated by anger and frustration. Some of the attacks can even be based on moral standpoints, such as attacks on gambling and pornography sites.

Anger motivated attacks can be person-to-person, rather than person-to-company such as in cyber-stalking and cyber-bullying. Cyber-stalking is a targeted cyber-attack on one person for reasons of anger, revenge or control. The term can also apply to a “traditional” stalker who uses technology to trace and locate their victim and their movements more easily³⁹. Cyber-stalkers aim to harass, embarrass and humiliate their chosen victim. Cyber-stalkers never reveal their identity to prevent any repercussions and to enjoy the fear and anxiety that an unknown attacker creates. Cyber-bullying occurs when a person is bullied, harassed, humiliated, threatened, embarrassed, or targeted in some way by another person using modern communication systems such as cellular phones (SMS/MMS) and Internet⁴⁰. An attacker can use cyber-bullying to air his/her grievances, hatred and anger. The reasons for this anger can vary, ranging from the victim offending the attacker to a victim’s race or religion. The methods used by cyber-bullies tend to be generally unsophisticated and often depend on the utilization of social networks.

Sexual Impulse

Sexual predators use; the availability of personal information, anonymity and sometimes unrestricted access to social network sites and the Internet in general, to identify and gather information on potential victims.

Pedophiles are the major criminals in this category as they prey on the naivety of children to the open approach they adopt when on social network websites. As at 2007, approximately 93 percent of all Americans between 12 and 17 years old are Internet users. One in five U.S. teenagers has received an unwanted request to engage in sexual activities or sexual talk, or to give out personal sexual information on the

web⁴¹. Pedophiles use chat rooms, social network services and instant messaging as sources for potential victims. These places are targeted as they encourage free sharing of information, communication with new people and provide anonymity to the users. Dr. Kimberly Young in her 2005 article entitled, Profiling Online Sex Offenders, Cyber-Predators, and Pedophiles wrote on the difference between virtual offenders and classic offenders:

“Virtual Offenders are more likely to suffer from an addictive disorder motivated by an attempt to use sexual fantasies as a way to escape problems in their lives, acknowledging the exploitative features and harm or pain they inflict. In comparison, Classic Offenders make a conscious attempt to use children for self-gratification driven by a need for power, dominance, control, revenge, or anger, denying the exploitative features and harm and pain they inflict”⁴².

Serial rapists use similar methods, however, the choice of website can vary. To find adults they target social networking websites and dating sights. Dating websites are especially good as they can do research and portray themselves as a perfect match for women who are eager to find love. The women using these websites can naively assume everything on a person's profile is true and make dates with predators. This method of acquiring victims allows the predator to entice the victim to him. The predator can control meeting location and time to create the best scenario for his/her escape.

The best defense against these types of attacks is awareness, as the attacks while utilizing technology are not technical, but based on social engineering. Potential targets must be made aware of the risks and informed of practices to safeguard themselves.

PROFILING

In order to defend against cybercrime and to enable law enforcement to identify and apprehend cyber-criminals, there needs to be an analysis of the motives and reasons why such attacks occur. This must be based on critical analysis of historical data to identify unique relationships between characteristics, weapons, targets, goals and behavioral patterns for different categories of cybercriminals. Profiling is the art and science of identifying relationships, which has in the past proven to be an invaluable tool for law enforcement. In the case of cyber-attackers, profiling has been based on five characteristics; level of technical expertise, level of disregard for the law/ ability to rationalize an unlawful act, tolerance to risk /need for the thrill and motive⁴³. Motive being a key factor in narrowing the profile and potentially making a case against an attacker. The possible motives for cybercrime that have been highlighted are money, emotion, sexual impulses, politics/religion and fun.

Profiling of cybercrime while generally the same as traditional crime may require a unique approach, as an understanding of technology must be meshed with knowledge of psychology, criminology and law⁴⁴. This unique approach would entail identifying key factors based on the aforementioned areas of study that are necessary

for developing a cyber-criminal profile. Table 1 is a generalized example of a sectional approach to profiling using the previously proposed motivation categories as the base of its construction. Other factors considered in the model are selection of victim, nature of attack, goals, technical resources and motivation. The motivation of the attacker is closely related to the selection of victims and modus operandi of the attacker. The motive of the attacker can dictate the type of attack utilized, whether he takes responsibility for the attack, the duration of the attack and the amount of damage done. The technological resources bring the digital aspect of cybercrime back into the profiling process. This factor deals with the level of technical skill and the sophistication of the cyber-weapon used. Directly or indirectly motives contribute to 75 percent of the cybercriminal profiling process. Therefore understanding the motives of cybercriminals [and criminals in general] is essential to any profiling effort.

Table 1

Sample Cybercrime Profiling Table Based on Motivation

Motivation Categories	Example of Attackers	Main Goal	Topography	Victim²
Financial	General criminal	• Economic gain • Acquisition of personal information	One to One	Individual
	Organized Crime Group	• Economic gain • Acquisition of personal information • Money laundering	One to Many	Individual
	Trusted Insider	• Unauthorized access • Financial gain	One to One	Private Organization
	Competitors	• Unauthorized access • Economic gain • Disruption of activities/Corruption of data	One to One	Private Organization
Political	Political Activists	• Sabotage adversaries • Reflect political tensions	Many to One	Political Websites
	State Actor	• Achieve Foreign Policy Objectives • Gain technical or military advantage	One to One	Private or Government Organizations
Emotion	Cyberpunks	• Thrill • Prestige	One to One	Private Organization
	Script Kiddies	• ‘Justice’ • Personal Enrichment retribution	One to One	Private Organization
	Stalker Pedophile	• Fulfillment of desires • To Identify victims	One to One	Individual
Ideology	Cyber-Terrorist	• To create fear and chaos • Intimidation	One to One	Private Organization
	Hacktivist	• Political/social change	One to One	Private Organization

² This information may occasionally vary based on the needs of the attacker.

CONCLUSION

In the 21st century, it seems that a growing community of cybercriminals has held the entire world at ransom. Their effect is destructive and extremely costly, with their targets including individuals, private organizations, government agencies and even nation states. Methods to identify attackers and potential attackers are essential to maintaining the rule of law in cyberspace and the physical world. As earlier highlighted, cybercrime at its core has similar motivations to conventional crime as the perpetrator is still human; only the medium for committing crime has changed. Therefore, just as with conventional crime, a comprehensive understanding of the contributing factors to cybercrime, its characteristics, the characteristics of the attackers and the weapons used and their relationship is critical to dealing with the scourge of cybercrime. This paper utilized traditional categories for the motivation behind committing crime, which were based on activity in the physical realm and mapped them unto cybercrime, which allowed a glimpse into the human aspect of cybercrimes.

Apart from that the works of Furnell (2001), Ngafeeson (2009), Shinder (2010) and Grzybowski (2012), previous work was biased towards classifications that focused solely on the technological aspect of cybercrime. The view of cybercrime presented in this analysis is designed toward a holistic view of cybercrime for law enforcement. The sociological view point presented in this work favors efforts of law enforcement to implement cybercrime prevention methods rather than just cybercrime security. The Routine Activity Theory proposes that the occurrence of crime depends upon the convergence of (i) a motivated offender, (ii) a suitable target, and (iii) absence suitable deterrence (barrier or guardian). While cybercrime is a sociotechnical phenomenon

the traditional approach has focused mostly on the technical aspect, which can only account for two of the factors considered in the Routine Activity Theory. Therefore, to have a holistic picture of cybercrime and to be able to create a truly comprehensive approach to dealing with cybercrime an analysis of the sociological aspect of the crimes should be undertaken. Understanding why cybercriminals actually commit the crimes may prove to be more beneficial in the fight against cybercrime than traditional approaches, which have so far fallen short. In criminal law, motive is a key consideration in any case, as it can prove plausibility in favour of the accused of the intent for committing a crime. Therefore, this categorization can serve as a valuable tool to legal professionals and lawmakers in building cases and developing legal frameworks for dealing with cybercrimes. The incorporation of the concept and theory behind this research may positively change the way law enforcement conducts investigations, looks at evidence and builds cases. This can be done by identifying how and to what degree traditional criminology theories can explain why persons commit cybercrimes. It can also provide the basis for further investigation of the factors that have led to an increase use of the cyberspace as a medium for criminal activity.

Quantitative analysis into motivation and other sociological variables, will aid in fully adapting traditional criminogenic theories in the creation of new cyber-centered theories that can overcome challenges of applicability unique to cybercrime such as; technical expertise, geographic distribution, asymmetric nature of attacks, attribution problems within the legal frame work or lack thereof. The use of quantitative analysis can also provide a medium to apply motivation to inductive profiling.

However, the problem with the use of quantitative methods in cybercrime research has been, and remains, the unavailability of information. A large portion of cybercrimes remains unreported or unnoticed by individuals and organization, which can potentially affect the legitimacy of data⁴⁵. Organizations in particular do not report incidents; as they fear negative financial repercussions due to loss of trust by investors and customers. Therefore, knowledge of the types of companies not reporting must be obtained, or measures implemented to encourage reporting to prevent the data obtained from quantitative measures being skewed. The latter option can be achieved by implementing a secure system for reporting cybercrime incidents that protects the identity of the reporting entities. This combined with communication with the organizations to emphasize the importance of reporting in the fight against cybercrime and future protection of their assets would prove effective. Since evidence gained in investigations can vary as it relates to different variables, it is essential that as many factors as possible are taken into consideration when developing a final profiling model.

---

¹Kristin M.Finklea, and Catherine A. Theohary. "Cybercrime conceptual issues for Congress and U.S. law enforcement".2012. [Washington, DC]: Congressional Research Service, Library of Congress. <http://www.cq.com/pdf/crsreports-4096596>

²Avinash Rajput, "Cybercrime".LokNayakJayprakeshNarayana National Institute ofCriminology and Forensic Science, Ministry of Home Affairs, nd.

³Comprehensive Study on Cybercrime [Electronic Resource]. Vienna: UNODC, 2013.

⁴Pierluigi Paganini, "The cybercrime Ecosystem, Resources,Motivations and Methods" Security Affairs. July 3. 2013. <http://securityaffairs.co/wordpress/tag/ponemon-institute>

⁵Rita Tehan, Cybersecurity: Authoritative Reports and Resources.Congressional Research Service.2013, <http://www.crs.gov>.

⁶Jill Aitoro,Determining the Motives for Cyberattacks Canbe Tricky.*Nextgov*. February 23. 2010, <http://www.nextgov.com/cybersecurity/2010/02/determining-the-motives-for-cyberattacks-can-be-tricky/46029/>.

⁷Kristin M.Finklea, and Catherine A. Theohary. "Cybercrime conceptual issues for Congress and U.S. law enforcement" ,pg 7.2012. [Washington, DC]: Congressional Research Service, Library of Congress. <http://www.cq.com/pdf/crsreports-4096596>

⁸Ibid

-
- ⁹ Paolo Buonanno, "The Socioeconomic Determinants of Crime: a Review of the Literature." University of Bergamo, 2006.
  - ¹⁰ Scott Newton, "Can Cyberterrorists Actually Kill People?." *SANS Institute InfoSec Reading Room*. Vancouver, 2002.
  - ¹¹ Carol Cratty, "FBI on Guard Against Terrorist Cyber Attacks." *CNN*. March 16, 2012, <http://edition.cnn.com/2012/03/15/us/cyber-attacks/index.html?iref=allsearch>.
  - ¹² Rachel Rudolph, "Understanding Cyber Warfare. From Cyber Warfare to Cyber Resistance." *Global Research*. November 28, 2011, <http://www.globalresearch.ca/understanding-cyber-warfare-from-cyber-warfare-to-cyber-resistance/27903>.
  - ¹³ Paula Newton, "Hezbollah and Cyber War." *CNN*. March 14, 2008, <http://edition.cnn.com/WORLD/blogs/security.files/2008/03/hezbollah-and-cyber-war.html>.
  - ¹⁴ Gabriel Weimann, "Cyber-Fatwas and Terrorism." *Studies in Conflict & Terrorism* 34 (10), 2011: 765–781.
  - ¹⁵ Tony Capaccio, "Al-Qaeda Seeks Cyber-Attack Skills, U.S. Official Says." *Bloomberg Businessweek*. April 25, 2012, <http://www.businessweek.com/news/2012-04-25/al-qaeda-seeks-cyber-attack-skills-u-dot-s-dot-official-say>.
  - ¹⁶ Council, United Nations Security. 2001. *Resolution 1373, 2001*.
  - ¹⁷ *Model Legislative Provisions Against Terrorism*. 2009. *Model Legislative Provisions Against Terrorism*. United Nations Office on Drugs and Crime.
  - ¹⁸ Dr Raymond Choo, "Cybercrime 101." , 2010: In, 1–29.
  - ¹⁹ Harry Sverdlove, "Cyber Attack at IMF – Why Motivations Matter." *Bit9*. June 12, 2011, <https://blog.bit9.com/2011/06/12/cyber-attack-at-imf-why-motivations-matter/>.
  - ²⁰ Michael Dahan, "Hacking for the Homeland: Patriotic Hackers Versus Hacktivists." , 2013: In, 51–57. International Conference On Information Warfare & Security.
  - ²¹ Douglas Morris and Lauren Langman, "Networks of Dissent: a Typology of Social Movements in a Global Age." Loyola University of Chicago, n.d.
  - ²² Francois Paget, "Cybercrime and Hacktivism." McAfee Labs, 2010.
  - ²³ Eric Sterner, "Hacktivists' Evolution Changes Cyber Security Threat Environment." *World Politics Review*. April 21, 2013, <http://www.worldpoliticsreview.com/articles/print/11864>.
  - ²⁴ Michael Dahan, "Hacking for the Homeland: Patriotic Hackers Versus Hacktivists." , 2013: In, 51–57. International Conference On Information Warfare & Security.
  - ²⁵ Ibid
  - ²⁶ J Nazario, "Politically Motivated Denial of Service Attacks." *Cryptology and Information Security Series* 3, 2009: 163–181.
  - ²⁷ Dr Bartosiewicz, "Cybersecurity in 2012-2015." , 2011: In. Novi Sad.
  - ²⁸ Jeffrey Carr, *Inside Cyber Warfare : Mapping the Cyber Underworld*. Sebastopol, CA: O'Reilly & Associates, 2011.
  - ²⁹ Eamon Javers, "Secrets and Lies: the Rise of Corporate Espionage in a Global Economy." *Georgetown Journal of International Affairs*. 2011, <http://journal.georgetown.edu/wp-content/uploads/53-60-FORUM-Javers.pdf>.
  - ³⁰ Alyssa Carducci, "Cyber-Hacking Is Latest Tool in Corporate Espionage." *Heartlander*, n.d., <http://news.heartland.org/newspaper-article/cyber-hacking-latest-tool-corporate-espionage>.
  - ³¹ "Symantec Intelligence Report: June 2012." 2012. "Symantec Intelligence Report: June 2012." Symantec.
  - ³² Zaiton Hamin, Zaiton. "Insider Cyber-Threats: Problems and Perspectives." *International Review of Law, Computers & Technology* 14 (1), 2002: 105–113.
  - ³³ "Consumer Sentinel Network Data Book CY-2012." 2013. "Consumer Sentinel Network Data Book CY-2012." Federal Trade Commission.
  - ³⁴ Pati Parthasarathi, "Cyber Crime." *Naavi*. Accessed April 25, 2013. http://www.naavi.org/pati/pati_cybercrimes_deco3.htm.
  - ³⁵ "Online Gambling: a Perfect Tool for Money Laundering." , "Online Gambling: a Perfect Tool for Money Laundering." *Bookmakers Review*. March 4, 2013. <https://www.bookmakersreview.com/gambling-news/online-gambling-perfect-tool-money-laundering/48289>.
  - ³⁶ Debra Shinder, "Profiling and Categorizing Cybercriminals." *Tech Republic*. July 19, 2010.

-
- ³⁷ David Kushner, "Machine Politics: the Man Who Started the Hacker Wars.." *The New Yorker*. May 2, 2012, http://www.newyorker.com/reporting/2012/05/07/120507fa_fact_kushner.
- ³⁸ Debra Shinder, "Profiling and Categorizing Cybercriminals." *Tech Republic*. July 19, 2010.
- ³⁹ Alexis Moore, "What Is Cyberstalking?." *About.com*. Accessed April 26, 2013, <http://womensissues.about.com/od/violenceagainstwomen/f/Cyberstalking.htm>.
- ⁴⁰ K Jaishankar, *International Perspectives on Crime and Justice*. Newcastle: Cambridge Scholars, 2009.
- ⁴¹ Amanda Lenhart and Mary Madden, "Teens, Privacy and Online Social Networks." *Pew Internet*. April 18, 2007. <http://www.pewinternet.org/Reports/2007/Teens-Privacy-and-Online-Social-Networks.aspx>.
- ⁴² Dr Kimberly Young, "Profiling Online Sex Offenders, Cyber-Predators, and Pedophiles ." *Journal of Behavioural Profiling* 5 (1), 2005: 1–18.
- ⁴³ Debra Shinder, "Profiling and Categorizing Cybercriminals." *Tech Republic*. July 19, 2010.
- ⁴⁴ Hemamli Tennakoon, "The Need for a Comprehensive Methodology for Profiling Cyber-Criminals." *New Security Learning*, 2013.
- ⁴⁵ Comprehensive Study on Cybercrime [Electronic Resource]. Vienna: UNODC, 2013.