International Journal of Computer Networks and Communications Security

VOL. 4, NO. 6, JUNE 2016, 165–176
Available online at: www.ijcncs.org
E-ISSN 2308-9830 (Online) / ISSN 2410-0595 (Print)

Cybercrime and Cybercriminals: A Comprehensive Study

REGNER SABILLON[1], JEIMY CANO[2], VICTOR CAVALLER[3], JORDI SERRA[4]

[1] Network and Information Technologies Doctoral Programme, Universitat Oberta de Catalunya (UOC), Barcelona, Spain

[2] Law Faculty, Universidad de los Andes (Uniandes), Bogota, Colombia

[3] Information and Communication Studies, Universitat Oberta de Catalunya (UOC), Barcelona, Spain

[4] Network and Information Technologies Doctoral Programme, Universitat Oberta de Catalunya (UOC), Barcelona, Spain

E-mail: [1]regners@athabascau.ca, [2] jcano@uniandes.edu.co, [3]vcavaller@uoc.edu, [4]jserrai@uoc.edu

ABSTRACT

The increasing expansion and diversification in the strategies and practices of cybercrime has become a difficult obstacle in order both to understand the extent of embedded risks and to define efficient policies of prevention for corporations, institutions and agencies. The present study represents the most comprehensive review of the origin, typologies and developments of Cybercrime phenomenon over the past decade so far. By means of this detailed study, this paper tackles the issue first describing and discussing former different criteria of classification in the field and secondly, providing a broad list of definitions and an analysis of the cybercrime practices. A conceptual taxonomy of cybercrime is introduced and described. The proposal of a classification criterion is used in conjunction with a cybercrime hierarchy derived from the degrees and scale of vulnerability and targets.

Keywords: *Cybercrime, Cybercrime taxonomy, Network-level Security and Protection, Security and Privacy Protection, Abuse and Crime Involving Computers.*

1 INTRODUCTION

The first historical events related to cybercrime, have its roots when the initial computer networks were set up and at the same time due to the growth of personal computing; these events marked an expansion of the cybercriminality. The pioneer hackers were conceived at the MIT (Massachusetts Institute of Technology) in 1960 and on November 20, 1963, they were mentioned by an MIT student (The Tech: MIT Student Journal -1963). Although, the term was meant to describe the fancy use to manipulate computers. As years passed by, the term acquired a different connotation; linked to cause damages to information systems and computers.

Einar Stefferud reported that in 1978, he sent the first electronic mail as spam. It was DEC that committed this abuse by using the ARPANET's distribution list (Advanced Research Projects Agency Network) to advertise a new computer – the "DEC-20".

Sweden was the first country to make a law for data protection called "Swedish Data Act of 1973", it states that data must be protected against all unauthorized access.

The United States of America was the second country to create a law to punish the cyber criminality; this act was introduced by Senator Abe Ribicoff and ratified as "Federal Computer Systems Protection Act of 1977". All these isolated events were crucial for the introduction of the Computer Forensics and Digital Forensics; both considered a science and an art. Robert Morris Jr. was the first cybercriminal on trial and sentenced the 26th of July 1989 under the "Computer Fraud and Abuse Act of 1986".

A recent report from the Internet Society presents interesting key statistics and trends [1]:

- There were 3 billion Internet users in May 2015
- Mobile Internet penetration will reach 71% by 2019
- 192 countries have implemented 3G mobile networks
- Nowadays the existing number of apps exceeds 1 million, which were downloaded more than 100 billion times

The cybercrime term was coined by Sussman and Heuston in 1995. Cybercrime cannot be described as a single definition, it is best considered as a collection of acts or conduct – these acts are based on the material offence object and modus operandi that affect computer data or systems [2]. The term cybercrime constitutes illegal acts where a digital device or information system is either a tool or target o simply a combination of both. The cybercrime expression can be used interchangeably either as computer crime, electronic crime, e-crime, high-technology crime, information age crime, cybernetic crime, computer-related crime or digital crime.

While the *"hacker"* term meaning has changed over the last decades, the conceptualization of the activities of this group is mostly seen as dark, evil, operating in underground environments and particularly with intentions to cause damage against society's information systems. The main agents in cybercrime activities are hackers. Their motives can be from just having personal fun – like script kiddies defacing websites and breaking access passwords, to the satisfaction of being recognized as an elite hacker by breaking cybersecurity and stealing from Fortune 500 Companies.

1.1 Classification

There are a lot of hacker categories; these categories include different terminology and iconography that create controversy over the computer attacker terms. The media and general public refer to people who are responsible for attacking and damaging computer systems as "hackers". But using the term hacker to label a cybercriminal or computer vandal denigrates the term as well the historic concept.

Most of hacker online activities are perfectly legal; the difference between hackers, hackers who commit crimes and cybercriminals rest upon their attitudes when a hacker accepts the activity and the motives.

1.1.1 Categories

The SANS Institute (2004) based on previous researcher's work have determined various categories and subgroups of hackers:

***White hats*:** These individuals work within the laws of the hacker ethic (to do no harm) or as security experts.

***Gray hats*:** This term was coined by L0pht – one of the best known old school hacking groups. These hackers are reformed Black Hats now working as security consultants.

***Black Hats*:** These hackers are motivated by power, anger or hate. They do not have any qualms to steal or destroy network data that they penetrate.

1.1.2 Classes

These classes of hackers are under both Black Hat and White Hat categories:

***Elite*:** They have the knowledge and skills of the highest level. This status can be gained by a particularly famous exploit, hack or longevity on the scene.

***Script Kiddies*:** The most scorned subgroup within the larger hacker community. These tend to be the least skilled and youngest members using the tools created by elite hackers.

***Cyber-terrorists*:** They use stenography and cryptology for exchanging information and sharing plots online. These hackers are considered to become the most serious of computer criminals.

***Disgruntled (ex) employees*:** one of the most dangerous, least publicized groups. These people believed they were owed special recognition for their corporate work and would take revenge for the lack of it.

***Virus Writers*:** This group tends to exploit weaknesses found by hackers, then code methods to execute computer flaws.

***Hacktivist*:** This name derives from combining the words 'activism' and 'hacking'. One of the fastest growing hacker subgroups, which are motivated to deface websites and launch Denial of Service (DOS) attacks to satisfy political, religious and social agendas.

The EC-Council (2014) has created a different taxonomy based on Hacker classes. They highlight the differences between regular hacking versus ethical hacking. This categorization includes eight different classes:

***Black Hats*:** Hackers with excellent computing skills that are attracted to malicious activities. Their motives are to cause damage, steal information, destroy data and earn money.

***White Hats*:** Individuals with hacking skills those act to protect networks in a defensive way. They work is corporate environments as security analysts.

***Gray Hats*:** Hackers that work both offensively and defensively at different situations.

***Suicide Hackers*:** Hackers that aim to bring down critical infrastructure for radical causes and are not afraid to go to jail. They are related to suicide bombers and are active member of cyber terrorism groups.

***Script Kiddies*:** The most unskilled hackers that are not well versed in hacking techniques. They tend to focus in getting high quantities of attacks rather than performing quality attacks.

***Spy Hackers*:** These hackers are on contract to penetrate and gain trade secrets of their employer's competitors.

***Cyber Terrorists*:** These could be people or organized groups that are motivated by political or religious motives to cause harm by disrupting large scale computer networks.

***State Sponsored Hackers*:** State sponsored hackers that are employed to damage other countries' networks and information systems.

Warren and Leitch (2009) have created an additional hacker category that was not considered before. The researchers have identified a sub group of hackers called "Hacker Taggers". These hackers like to deface websites with the intention of leaving a 'hacker tag' or 'calling card' behind. This tag or card is updated to show hacker's individual scores.

The website Zone-H (www.zone-h.org) contains an archive of website defacement history since 1999.

In terms of hacker categories and classes, we remark that there is not a globally accepted categorization of hacker groups nor classes. While many organizations have agreed on certain categories, that intend to group hackers by their motives and actions. We agree that the most common categories are black, grey and white hat hackers and any resulting sub-categorizations are based on specific motives, propaganda, hacktivism, political or religious reasons.

1.1.3 Motivation

Describing a typical cybercriminal stereotype and its motives is almost impossible, mostly because cybercrime agents act based on one or several motives.

Some motives entail curiosity, fun, satisfaction, publicity, manipulation, destruction, revenge, ego gratification, hacktivism, nationalism, radicalism, religion, politics, and financial benefit.

In fact, the SKRAM (Skills, Knowledge, Resources, Authority, Motivation) model [3] can calculate the threat potential of cybercriminals using their skills, knowledge, resources, authority, intensity of motives and countervailing information assurance linked on technological and human factors.

The formula is (S*K*R*A*M) / IA where these factors have impact on the amount and time under certain circumstances of the cybercriminal's capabilities.

2 CYBERATTACKS

We base our study on previous research work (*Table 1*) from practitioners, scholars and industry experts. Arief et al. previously studied cybercrime on two different perspectives: Part 1 from the attacker's side [4] and Part 2 for defenders and victims [5]. Chawki et al. [6] focused on cybercrime and its management issues. Cardwell et al. studied theft of intellectual property, damage of corporate networks, financial fraud, hacker system penetration and execution of viruses and worms. Britz [7] introduced traditional computer crime, contemporary computer crime, identity theft, identity fraud, cyberterrorism and technological organized crime. Mc Quade, III categorized cybercriminals based on the nature of their cybercrimes.

Table 1: Previous studies on cybercrime and cyberattacks

Authors	Insight about their taxonomy
Arief, Adzmi and Gross (2015)	Taxonomy about stakeholder's involvement: attackers, defenders and victims
Chawki, Darwish, Khan and Tyagi (2015)	They studied the cybercrime fundamentals, computer systems a targets, computer systems as tools, content-related offences and cyberspace anonymity including privacy, security and crime control
Cardwell et al. (2007)	Comprises the 3 Ts: tools to commit crimes, targets of the victim and tangential material to the crime.

	They categorized cybercrime using insider and external attacks.
Britz (2013)	Typology included early hackers, theft of components, neotraditional cybercrime, identity theft/fraud, cyberterrorism and its links with the organized crime
McQuade, III (2006)	Categories of IT abusers and cybercriminals are negligent users, traditional criminals, fraudsters, hackers, malicious code writers, media pirates, harrasers, cybersex offenders, academic cheats, organized criminals, freelance spies and cyberterrorists

Our cyberattack and cybercrime taxonomies are established on current threats, vulnerabilities, hacker subculture, risks, impact, technology and human factors. With those principles in mind, our efforts must be oriented towards the safeguarding of the cybersecurity triad that encircles confidentiality, integrity and availability.

Nowadays, cyber vulnerabilities are exploited using simple, sophisticated or a combination of several cyberattacks. In this section, we present the most common type of cyberattacks [8], we need to understand that as technology evolves new risks and threats will lead to more advanced Techniques, Tactics and Procedures (TTP) to system's hacking.

2.1 Advanced Persistent Threats (APT): The term Advanced Persistent Threat was coined in 2005 by an USAF security analyst [9]. According to the US National Institute of Standards and Technology (NIST), an APT is an adversary that possesses sophisticated levels of expertise and significant resources to create opportunities to achieve its objectives using multiple attack vectors. It pursues objectives over an extended period of time; adapts to efforts of the defenders and maintains an adequate level of interaction aligned with its objectives. The attack cycle encircles target selection, target research, target penetration, command and control, target discovery, data exfiltration, intelligence dissemination and information exploitation.

***2.2 Arbitrary/remote code execution*:** Attackers use techniques to install malware remotely in order to take partial or complete control of a system.

***2.3 ARP poisoning*:** Address Resolution Protocol poisoning misleads interconnection devices about the real MAC of a machine. ARP contains only two types of messages: ARP request and ARP reply. Attackers create ARP reply packets using spoofed MAC addresses to poison ARP cache on any network system. VLAN segregation prevents this type of attack.

***2.4 Bluejacking*:** It is the process of sending text messages using a private Bluetooth device without the owner's consent. In addition to text messaging, some Bluetooth devices can include sound. The best security strategy is to operate the device in a non-discovery mode.

***2.5 Bluesnarfing*:** Unauthorized access to a Bluetooth device or data theft from any Bluetooth connection. This attack will take place as long the device is on and set to discovery mode. Linux users can launch this type of attack using hcitool and ObexFTP tools.

***2.6 Buffer overflow*:** This usually happens whenever an application receives more input than it can handle. The result is a system memory error that exposes a vulnerability that later can be exploited to write malicious code. Normally the sequence attack is primarily causing the buffer overflow, then is sending a long NOOP (No Operation) command, inserting the malicious code and finally by triggering the code execution.

***2.7 Client-side attacks*:** This type of attack can be launched using a client application aiming to access specific servers or databases. This can be avoided if proper input validation and stored procedures are in place. Client-side attacks are based on transitive trust access that allows forest trust relationships in all Active Directory domains.

***2.8 Cookies and attachments*:** Cookies can store web browsing history and sensitive data including usernames, passwords and session IDs that are instrumental for additional attacks like session hijacking. Malicious attachments can trigger malware attacks like viruses, Trojans and worms.

***2.9 Cross-site Request Forgery (XSRF)*:** Attackers fool users by creating malicious HTML links and redirecting the victims to perform specific actions. A security measure is to create expiration cookies and to prevent automatic log on.

2.10 Cross-site Scripting (XSS): This attack redirects end users to malicious webpages, by encoding <or>, <img>, <and> tags and embedding HTML or JavaScript code into websites or emails. Once the link is open then the code will run on the user's computer. Local cookies can be read after the script is executed. Web developers must block HTML and JavaScript tags by hardening input validation on webpages.

2.11 Denial-of-Service (DoS): Attack that inhibits legitimate users from accessing computer services. Normally DoS target connectivity or network bandwidth by overflowing server traffic, resources, nodes or services. Some techniques to launch the DoS attacks include SYN flood, bandwidth, service request, ICMP, P2P, permanent DoS, smurf, app level and buffer overflow.

***2.12 Directory/command injection*:** These attacks use commands to manipulate an application via the Operating System or the deletion of directories, subdirectories or files. A good security measure is to implement input validation.

2.13 Distributed Denial-of-Service (DDoS): DDoS are launched using several zombie computers (botnet- derived from roBOT NETwork) attacking a specific target. During a DDoS the target computer will sustain extreme network traffic, memory and processors usage. To detect outbound traffic, use the command line tool **netstat -a**

***2.14 DNS poisoning*:** Domain Name System poisoning is an attack that modifies or corrupts cached DNS results. The major risks are the propagation of poisoned DNS information to the Internet Service Providers and be cached in their servers.

2.15 Domain Name kiting: This practice allows attackers to register domain names and delete them after the five-day free trial. During the free period, domain tasting will generate traffic and likewise generate revenue without paying for the domain registration.

***2.16 Evil twin*:** Rogue access point attack that configures a WAP (Wireless Access Point) with the same SSID (Service Set Identifier) of a valid WAP. Attackers set these devices in public places with free Wi-Fi. Sensitive information is stolen from the users that connect to the evil twin.

***2.17 Flash cookies*:** Because Adobe Flash cookies can be set to never expire; they represent a high risk to steal user's browsing history. Flash cookies are normally 5 MB in comparison to regular cookies that only store 1,024 bytes of information. Flash cookies are able to recreate deleted cookies.

2.18 Fuzz Testing: It is used to detect system vulnerabilities that can be later exploited. This attack transmits strings of data from scripting to specific applications.

***2.19 Hash injection*:** It is an attack that injects an altered hash to authenticate into a local session in order to access network resources. Attackers will log onto the domain controller, accessing the Active Directory and manipulating domain accounts.

***2.20 Header manipulation*:** Flags are modified within data packets granting legitimate rights to attackers. Dual authentication prevents manipulating user's data.

***2.21 ICMP flooding*:** DoS attack that sends Internet Control Message Protocol (ICMP) packets with spoof source addresses so TCP/IP requests stop. Once the ICMP threshold is reached the router no longer accepts the ICMP echo requests.

2.22 Information disclosure: These attacks allow perpetrators to obtain valuable information about a system. Some examples include revealing passwords, shoulder-surfing, loss of thumb drives, laptop theft, message insecurity over HTTP, sharing of confidential policies, data leakage and social engineering information disclosure.

***2.23 Integer overflow*:** This attack is the result when an arithmetic operation exceeds the maximum value of an integer used for storage. This exploit can be used for buffer overflow, infinitive loops and data corruption.

***2.24 IV (Initialization Vector) attack*:** This exploit takes place on Wi-Fi networks using the WEP (Wired Equivalent Privacy) security protocol. WEP has known vulnerabilities. The attackers use packet injection for cracking the small IV for keys and obtaining the encryption key.

***2.25 Jamming interference*:** This attack can be part of a major Wireless Denial of Service (WDoS) attack. Attackers use malicious nodes to block access to the medium and likewise interfere with wireless or wired reception. Sophistication increases from continual transmission interference to exploiting protocol vulnerabilities.

***2.26 Keylogger attack*:** This can be a hardware device or a small program that records user's keystrokes or screen content. If it is a physical device, the attacker must remove it in order to access the information. On the other hand, if the hidden program was installed on the victim's

computer – its DLL (Dynamic Link Library) file will record all keystrokes.

***2.27 Lightweight Directory Application Protocol (LDAP) injection*:** This attack targets Active Directory accounts so can be modified using LDAP commands.

***2.28 Malicious add-ons*:** We have to be very careful about any additional add-ons that the browsers will install on our computers. There have been cases in the past that browser add-ons installed malware on the client computers. Some measures include running additional scans, do not download from compromised sites and keep system with the latest security patches.

***2.29 Malicious insider threat*:** An insider attack using valid system access credentials can compromise data confidentiality. Motives include revenge, financial gain and industrial espionage. Insider threats are very difficult to detect but a mix of controls can be implemented like least privilege, proper segregation of duties, auditing, enforcement of legal and security policies, restricted access and critical data backup management.

***2.30 Malware attacks*:** Malicious software that is installed through different devious ways. There are several categories of malware, the most common are viruses, worms and Trojan horses.

2.30.1 Virus: Malicious code that replicates by itself and needs execution in order to cause damage.

2.30.2 Worm: Self-replicating malicious code that spreads across the network without intervention or execution.

2.30. 3 Trojan horse: Trojans hide within a valid application that will get activated upon certain actions. These programs can even disable firewalls, create backdoors, activate botnets, generate fake traffic and delete system files.

2.30.4 Logic bomb: Malicious scripts that will activate for a particular event. Normally, they are programmed to destroy the operating system, deletion and formatting of all network drives.

2.30. 5 Rootkits: Programs that hide other malware by modifying the operating system. Some rootkits are at the boot loader, library, hardware, application, firmware, kernel and hypervisor levels.

2.30.6 Spyware: This program gathers sensitive information about the user.

2.30.7 Rogueware: These programs are also named scareware, the malicious programs masquerade as a security application and send messages of malware infection. After a system scan or trial expiration, users get asked to pay for a full version.

2.30.8 Ransomware: Extortive malware that locks user's data in order to get payment for unlocking the data.

2.31 Man-in-the middle (MITM): This type of attack allows active interception of network traffic and sending malicious code to the client's machine. Kerberos prevent MITM attacks by enforcing authentication.

***2.32 Misconfiguration attacks*:** These attacks take advantage of wrong, default or compromised configurations to access systems, networks, computers, servers, mobile devices or interconnection devices.

2.33 Near field communication (NFC): There are a few attacks under NFC including eavesdropping, data corruption and smartphone viruses. NFC devices can communicate if the separation is four centimeters or less. The biggest risk is card skimming due to the fact when mobile card readers are used to complete the online payments. NFC channels are also vulnerable to MITM attacks.

***2.34 Packet sniffing*:** Attackers use protocol analyzer or sniffer programs like Wireshark, TCPDump and Sniff-O-Matic to capture and track network packets. Unencrypted data is the most vulnerable when using sniffers – captured packets can easily be read and analyzed data can also be used to plan further cyberattacks.

***2.35 Password attacks*:** These attacks use different techniques to crack server, network device, systems or user passwords. Weak passwords can be avoided if they use a long combination of capital/ small case letters, numbers and special characters. Cracking techniques include brute force, rule based, dictionary, hybrid and syllable attacks. Some password cracking tools are L0phtCrack, John the Ripper, Cain and Abel, Passscape and Aircrack.

***2.36 Pharming*:** This type of attack aims DNS servers; it is particularly a DNS poisoning attack that redirects traffic to a fraudulent website. Cyber crooks can take advantage of this by stealing confidential information of users.

***2.37 Privilege escalation*:** When hackers penetrate systems, they normally have limited access accounts and want to obtain full privilege accounts like super admin accounts. Elevated rights and

permissions of attackers allow them to gain additional controls and remain unnoticed in the target system.

2.38 Rainbow attack: Attackers check the stolen password validity during this type of attack. By using cryptanalysis techniques, the time-memory trade off calculates memory information, inserting the password hash table, comparing and matching passwords until they are cracked.

2.39 Replay attack: Attackers replay data between communication sessions. Using the data, they can impersonate an user to obtain information. Kerberos block this type of attack using time-stamped tickets.

***2.40 Rogue access points*:** Counterfeit WAPs are connected to networks to capture traffic. This rogue device will easily grant access to unauthorized users using wireless and wired networks of the victim.

***2.41 Session hijacking*:** This process seizes an active network or application session. By intercepting and taking control of an user's session, the attacker inserts malicious code to target server afterwards. Packet interception happens at the network level and HTTP session takeover at the application level in OSI model. Some prevention measures against session hijacking include the use of Secure Shell (SSH), HTTPS, log-out functionality implementation and data encryption.

***2.42 Shrink wrap code attacks*:** These attacks are aimed at applications immediately after its initial installation. The most common vulnerability is to exploit default code from libraries.

***2.43 Smurf attack*:** A DoS attack that spoofs the source host to flood the target computer with ping replies.

***2.44 Social Engineering*:** Hackers use social tactics to persuade people to reveal sensitive information that can be later used for malicious actions. Social engineering types include using human interaction, computers or mobile devices.

Attackers normally pose as legitimate users, VIP executives or technical support analyst to commit their attacks. Best anti-social engineering strategies are education, security awareness training and enforcement of IT security policies.

***2.45 Spear phishing*:** This attack targets a specific user or a group of users. Normally uses an email that seems legitimate to ask for some wire transfer already approved by a top executive within a company.

***2.46 Spim*:** Spam instant messaging targets instant messaging apps such Yahoo Messenger, WhatsApp and Line. The attackers need mobile number confirmation if the users click the link. Best way to deal with Spim is to ignore the messages and delete them.

***2.47 Spoofing*:** Cyberattacks can use spoofing in many ways, from changing IP addresses to changing Media Access Control (MAC) addresses to email address by hiding the attacker identity.

***2.48 SQL injection*:** These attacks are the highest web vulnerability impacts on the Internet. A flaw in the coding of a web application is exploited to allow additional data entry to generate unique SQL statements. Many relational databases are vulnerable to this attack including DB2, MySQL and SQL SRV. These attacks can avoid authentication, trigger code execution and affect data integrity.

***2.49 SYN flooding*:** Common DoS attacks use SYN to flood servers. It is based on the Transmission Control Protocol (TCP) handshake process that overflows the normal three-way handshake using SYN and ACK packets between hosts. Attackers never send the ACK part and otherwise they keep sending multiple SYN packets to get several half-opened connections causing a system crash.

***2.50 Transitive access*:** This access involves a trusted relationship within a network that can be exploited to attack core systems. Client-side attacks use transitive relationships whenever an attacker cannot aim a direct cyberattack.

***2.51 Typo squatting*:** This is a form of cybersquatting that reroutes users to malicious websites. Active domain names with typographical errors are created, registered as valid URLs and then uploaded as alternate websites to infect users with malware.

***2.52 URL hijacking*:** This attack is also known as Man-in-the-Browser attack. It triggers a Trojan to hijack the communication between the browser and the libraries. The extension files from the Trojan convert the Document Object Model (DOM) interface and modify the user values.

***2.53 Vishing*:** This attack uses Voice over Internet Protocol (VoIP) or a phone system calls to trick users to give personal information in a similar way to phishing attacks. Attackers can spoof caller IDs to masquerade a phone call within a company. Personal information is at risk if the user provides the required information to validate some kind of financial transaction.

***2.54 War chalking*:** This technique is used to place special symbols on sidewalks or walls indicating an open Wi-Fi network.

***2.55 War driving*:** Attackers drive around to discover wireless networks for future exploits. Cantennas (Open-ended metal can antennae) are used to detect Wi-Fi networks.

***2.56 Watering hole*:** This attack identifies an organization website, exploits web vulnerabilities and installs malware that attacks silently the users.

***2.57 WEP/WPA attacks*:** These Wired Equivalent Privacy/ Wi-Fi Protected Access attacks use cracking tools to break 802.11 WEP secret keys. 40-bit to 512-bit keys can be cracked from captured data packets.

***2.58 Whaling*:** Whaling is a spear phishing attack that aims upper management executives. This attack targets a top executive by name using some kind of legal subpoena or customer complaint.

***2.59 Wire sniffing*:** This is a form of an active or passive wiretapping attack that monitors data traffic or alters data packets as required. Some vulnerable protocols to sniffing are HTTP, IMAP, Telnet, POP, FTP, SMTP and NNTP. Some measures to defend sniffing include physical restrictions, encryption, use of static IP addresses and IPv6 configuration.

***2.60 WPS attacks*:** Wi-Fi Protected Setup use buttons to connect to wireless networks and a secure WPA link. This Pin attack sets up a brute force method to crack into a WPA wireless network. Some countermeasures include disabling WPS or updating the access point firmware.

***2.61 Xmas attack*:** The Christmas tree attack is a port scan type used as a reconnaissance attack and the gathered information is crucial for further cyberattacks. The particular features are the inclusion of bit sets and flags in the TCP packet header that will trigger responses about open ports.

***2.62 XML injection*:** eXtensible Markup Language injection attacks are similar to SQL injection attacks. Major vulnerabilities include code insertion to input or export database data. In addition, XPath the XML query language can be entered using query statements for retrieval or modification of data.

***2.63 Zero day*:** This attack exploits undisclosed software vulnerability that the vendor has not yet created a security patch to fix it. Best action plan against zero day vulnerabilities is to limit the amount of active protocols and services.

3 A TAXONOMY OF CYBERCRIME

Some relevant previous studies from ITU [10] and ENISA [11] have categorized typologies of cybercrime. We present a comprehensive taxonomy (*Figure 1*) that has classified cybercrimes in our cyber era.

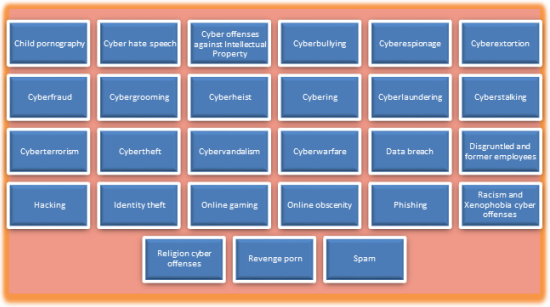

Fig. 1. A Cybercrime taxonomy

3.1 Child pornography: Illegal online pornography involves the participation of minors in sex activities. Some illicit online activities include exposing children in pornographic productions, sex exhibition, cybersex, prostitution, sex slavery, image and video distribution, chats, dating sites, Webcam Child Sex Tourism (WCST), sex toys, phone sex services and sex shows. Pornographers use digital software to merge images involving minors – this is known as morphing. Terres de Hommes Netherlands [12] fights children sexual exploitation; They created the 10-year old virtual Filipino girl called Sweetie- this project identified 1,000 predators from 71 countries using 19 chat rooms – These pedophiles were handed over to Interpol. 20,172 predators tried to engage with Sweetie. Sweetie 2.0 continues the fight against WCST.

***3.2 Cyber hate speech*:** Any form of online hate expressions that affect social rights, liberties and freedom of expression. Online hatred can target races, religions, nationalism, ethnic groups, countries, individuals, groups, minorities, migrants, gender identity, disabilities, national origin, political parties, sport teams, sexual orientation, youth, old people, children and animals. Some international agencies are fighting against cyberhate and some countries have created laws as well.

***3.3 Cyber offenses against Intellectual Property*:** Any cyber tort that infringes the protection of patents, trade secrets, trademarks and copyrights. More related to networks and computer security, the list will expand to software, databases, digital content, algorithms and raw data.

3.4 Cyberbullying: This involves the use of communication technologies to harass people. Cyber harassment mostly affects children and teenagers but can also target adults. Some forms include cyber extortion, distribution of embarrassing pictures, delivery of threatening messages, cyberbashing to mock people and impersonating victims. Parents can document the cyberbullying evidence, report to schools and local police.

***3.5 Cyberespionage*:** Acts that involve exfiltration, unauthorized access, interception and acquisition of data. Freelance spies utilize spyware, keyloggers, surveillance methods, data traffic interception, event recording and communication monitoring.

***3.6 Cyberextortion*:** Attackers will harass victims in order to avoid cyber damage. Cybercriminals will demand money for financial gain to avoid computer-related threats. A typical attack takes place using ransomware and asking the victim for a Bitcoin payment.

***3.7 Cyberfraud*:** Online fraud or forgery does exist in many possible ways. Victims are tricked using digital technologies. Some examples combine online auctions, stock fraud, credit card fraud, telemarketing fraud, false advertising schemes, false damage claims, insider trading, cyber smear campaigns, ad hoc fraud, computer hoaxes, click fraud, Ponzi/pyramid schemes, lottery/sweepstakes and contest scams, get-rich-quick schemes, Nigerian scam, ringtone scam, missed call scam, text message scam, SMS trivia scam, health scam, emergency scam, dating scam, job scam, small business scam and service scam.

***3.8 Cybergrooming*:** This online conduct allows a pedophile to build a relationship with the victim in order to gradually engage in sexual molestation. Once the offender gains the victim's trust, he will escalate using texting and phone calls containing sexually explicit material.

***3.9 Cyberheist*:** This cybercrime involves a large scale theft from banks or financial institutions. Malware, hacking or phishing techniques are normally part of the crime. The theft takes place using e-banking transactions, e-payments, inflating bank accounts and stealing cash from ATMs.

3.10 Cybering*:* This involves a series of online sex behaviors to stimulate children in a sexual way. The offenders exchange texting, images and video clips with their victims. Cyber child molesters access online communities, chat rooms, games and virtual worlds.

***3.11 Cyberlaundering*:** Cybercrime that comprises financial transactions using funds from criminal activities. Cyberlaundering is based on e-payments, digital money and illegal hardcash that is converted to illegal e-money.

***3.12 Cyberstalking*:** Online activities used by perpetrators to monitor people without their consent. This illegal activity involves online and offline tasks to intimidate, blackmail or any unlawful motive against their victims. The best way to prosecute the attackers is gathering all evidence to support a police case.

***3.13 Cyberterrorism*:** Cyberterrorists may carry terrorism activities exploiting computer vulnerabilities that will impact society in metropolitan or regional areas. Attackers are motivated by political, religion, hacktivism or personal matters.

3.14 Cybertheft: Cybercriminals seek financial profit by stealing and selling information in every possible way. The dark web is where most of the stolen information is for sale, the most common sold goods are credit card numbers, online auction credentials and bank account numbers.

***3.15 Cybervandalism*:** Vandalism that takes place using computer technology. The most common attacks are website defacement, malware to delete data, DDoS and social media account hijacking.

***3.16 Cyberwarfare*:** Attacks in cyberspace that are aligned with a specific military operation or a national cybersecurity strategy to attack another nation's cyberspace. These operations have a military connotation that are led by commanders and executed by government cyber warriors.

***3.17 Data breach*:** Disclosure of data or information that breaks confidentiality that leads to the distribution in the public domain. The leakage can occur by insider agents or hacker attacks. Damages can affect or trigger corporate reputation, financial losses, lawsuits, share prices, fraud and physical assets.

3.18 Disgruntled employees *and former employees*: These people will take revenge by compromising their employer or former employer's information systems. Some actions include theft of intellectual property using steganographic applications, install malware or backdoor programs, obtain unauthorized access and damage critical data.

***3.19 Hacking*:** Hacking becomes illegal once is used for unauthorized access to computer systems. Cybercrime is consummated once criminal hacking

takes place. Illegal hacking activities are usually part of organized crime networks, specific motives and a high degree of sophistication.

***3.20 Identity theft*:** This crime is the theft of someone's identity; the attacker pretends to be a different person to gain financial benefits. John Sileo- a successful entrepreneur was a victim of identity theft that caused his business bankruptcy and two years of his life to stay out of prison. Identity theft leads to identity fraud that exploits additional crimes like financial identity theft, business identity theft, criminal identity theft and money laundering.

***3.21 Online gaming*:** Online gaming and gambling are targets of cybercriminals. Hackers can steal user's personal information using malware, DDoS, phishing, black hat search engine optimization and webshell creation. Online gaming can also lead to cyberbullying of users. Factors like online casinos accessibility, 24/7 operations, minor's access and e-banking can easily lead to addictions, bankruptcy and cybercrime operations.

***3.22 Online Obscenity*:** Online pornography may not be illegal on the Internet but it may twist the concept that some sexual relationships are acceptable by society. Youth audiences are more vulnerable to this phenomenon; online obscenity offends and affects the morality of the audiences. USA protects minors with laws like the PROTECT Act and the Child Online Protection Act.

***3.23 Phishing*:** Fraudulent process that steals confidential information from end users. Phishing normally involves the use of fake websites. Phishers configure a universal man-in-the-middle phishing kit to activate a real time URL that interacts with a valid website.

***3.24 Racism and Xenophobia cyber offenses*:** Distribution of online material to discriminate, insult or threaten against groups or individuals based on race, ethnicity, culture, minority, colour, national descent, country of origin and dislike of foreigners.

***3.25 Religion cyber offences*:** Coming from one of the most dangerous forms of terrorism – the religious terrorism, religious cyber offences deliver hate speech against other religions and their followers. Adepts claim that they are empowered by their Gods and their actions are justified by the scriptures. The Cyber Jihads from the Islamic State (IS) are a radical group in charge of disseminating propaganda and censorship against other religions.

***3.26 Revenge porn*:** This cyber felony is the act of distributing sexual material of a victim without their consent. This is very common between disgruntled former partners that seek revenge or hackers that are blackmailing their victims seeking profit. As a result, victim's lives can be ruined, losing their jobs or the inability to obtain a new one. Google will respond to victims of nonconsensual pornography (NCP) to remove the content from search engine results.

***3.27 Spam*:** Unsolicited junk messages, images and advertisements are sent on every possible electronic way including email, blogs, search engines, instant messaging (IM) and smartphones. Spammers use botnets and virus infected networks to distribute spam.

4 THE DEEP WEB

The Deep Web is the core of the online underground criminal action; standard web browsers cannot access it neither search engines can index its content. A big component is the Dark Web, some systems include Freenet, TOR and Invisible Internet Project (I2P). The Dark Web requires very sophisticated tools to access it as most of the site owners wish to keep everything hidden.

The Tor (The Onion Router) browser is used to access the Deep Web; the browser allows anonymous surfing and it can hide your IP address with a different one.

The Deep Web is the cybercriminal's paradise – they can sell and buy malware, ransomware, crimeware, illegal drugs, weapons, stolen accounts, passports, driver's license, identity cards, credit cards, deal with cyber-laundering and the list goes on [13].

5 LESSONS LEARNED

Cybercrime is a complex and vast phenomenon; the proliferation of mobile devices, Wi-Fi networks and the Internet openness has increased the expansion of cyberattacks, the cybercriminality and the cyber victimization.

Protection against cybercrime starts at taking personal measures for protection and then escalates to organizational, societal, corporate, national, military and international levels. Defense in depth of cybersecurity at all levels will minimize, prevent and decelerate cyberattacks. Technology by itself is not enough, the integration of other fields like training, awareness, social aspects, culture, laws, prosecution and international cooperation are needed to blend with technical solutions to tackle cybercrime.

The creation of national governance to fight cybercrime, International cooperation to prosecute cybercriminals, the hardening of laws for prosecution, additional academia research and a participating cybersecurity industry are just some areas to be improved.

6 LESSONS TO BE LEARNED

The following five lessons establishes a reference learning plan in advance and create the ideal environment when reality becomes a process of conquest of existing paradigms in security and control:

Lesson 1 complements access control with use control.

Lesson 2 complements access control; to whom, to what resources and what permissions are required by considering the user location.

Lesson 3 complements the Return on Investment (RoI), with return for inclusion (reveals the benefits achieved in the company for applying security and control practices)

Lesson 4 balances the fear, uncertainty and doubt, with facts, observations, anecdotes and metaphors.

Lesson 5 complements the vision of known risks (feedback) with a vision of latent and emerging risks (feedforward) [14].

7 REFERENCES

[1] Internet Society (2015). "Global Internet Report 2015: Mobile Evolution and Development of the Internet". Geneva, Switzerland<http://www.internetsociety.org/globalinternetreport/assets/download/IS_web.pdf >

[2] United Nations Office on Drugs and Crime - UNODC (2013). "Comprehensive study on Cybercrime". Vienna, Austria <https://www.unodc.org/documents/organizedcrime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf>

[3] McQuade, III, S. (2006). "Understanding and managing cybercrime" (pp118-124; 132-133). Boston: Pearson/Allyn and Bacon.

[4] B. Arief, M.A. Bin Adzmi, and T. Gross, "Understanding Cybercrime from Its Stakeholders' Perspectives: Part 1— Attackers," IEEE Security & Privacy, vol. 13, no. 1, pp. 71–76.

[5] B. Arief and M.A. Bin Adzmi, "Understanding Cybercrime from Its Stakeholders' Perspectives: Part 2— Defenders and Victims," IEEE Security & Privacy, vol. 13, no. 2, pp. 84–88.

[6] Chawki, M. et al. (2015). "Cybercrime, Digital Forensics and Jurisdiction". New York: Springer International Publishing.

[7] Britz, M. (2013). "Computer Forensics and Cyber Crime". Third Edition. Upper Saddle River: Pearson.

[8] Gibson, D. (2011). "CompTIA Security+: Get Certified get ahead". Charleston, S.C.

[9] ISACA (2013). "Advanced Persistent Threats: How to Manage the Risk to Your Business" (pp 11-46). Rolling Meadows, Illinois.

[10] International Telecommunication Union – ITU (2014). "Understanding cybercrime: phenomena, challenges and legal response" (pp. 12-42). Edited by Marco Gercke. Geneva, Switzerland.<http://www.itu.int/ITU-D/cyb/cybersecurity/docs/CybercrimelegislationEV6.pdf>

[11] European Network and Information Security Agency – ENISA (2014). "ENISA Threat Landscape 2014" (pp. 14-39) Heraklion, Greece.<https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape/enisa-threat-landscape-2014/at_download/fullReport >

[12] Terres des Hommes Netherlands (2013). "Webcam Child Sex Tourism: Becoming Sweetie: A novel approach to stopping the global rise of Webcam Child Sex Tourism". The Hague, Netherlands. <https://www.terredeshommes.nl/sites/tdh/files/uploads/research_report.pdf>

[13] Trend Micro (2015). "Below the Surface: Exploring the Deep Web". Forward-Looking Threat Research Team. TrendLabs.< https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_below_the_surface.pdf >

[14] Cano, J. (2016). "Cinco lecciones por aprender en seguridad y control. Un marco de acción transdisciplinar desde la inevitabilidad de la falla". IT-Insecurity blog. <http://insecurityit.blogspot.com.co/2016/01/cinco-lecciones-por-aprender-en.html >

AUTHOR PROFILES:

Regner Sabillon
C|CISO, ITIL, CGEIT, CRISC, ISO 27001 LA, I.S.P., ITCP
MBA, M.Sc.
Ph.D. Candidate at Network and Information Technologies Doctoral Programme, Universitat Oberta de Catalunya (UOC), Spain, Canadian researcher in Cybersecurity, Cyber law, Cyberforensics and Cybercrime areas. Instructor at Athabasca University, Canada and ICT specialist with more than 20 years of experience

Jeimy Cano, Ph.D., CFE
Dr. Jeimy Cano is a Law Faculty Distinguished Professor at Universidad de los Andes (Uniandes) in Bogota- Colombia, a researcher and founder member of Research Group on electronic commerce, telecommunications and computing.

Victor Cavaller, Ph.D., M.Sc.
He is a Professor in the Department of Information and Communication Sciences at the Open University of Catalonia (UOC) and in the Faculty of Business at the Universitat Abat Oliva CEU, Spain.

Jordi Serra, Ph.D.
Jordi Serra holds a Ph.D. in Computer Sciences and is a Professor at the Master's degree in Information and Communication Technology Security at the Open University of Catalonia (UOC).
Researcher at KISON group. His research interests are information security, malware, hacking, steganography and copyright protection.