An Updated Taxonomy for Characterizing Hackers According to Their Threat Properties

Sara L.N. Hald, Jens M. Pedersen

Department of Electronic Systems, Aalborg University, Denmark

slh@es.aau.dk, jens@es.aau.dk

Abstract— **The objective of this paper is to give an up-to-date terminology for and categorization of hackers on the Internet, and to characterize each category of hackers by their threat properties. To be able to prioritize defense efforts, security experts need an accurate taxonomy of attackers for the production of detailed and precise threat assessments. We take an existing taxonomy for hackers and update it to correspond to the terminology used by hackers and security experts. Also, the categories of hackers are updated to reflect the threat properties demonstrated in recent attacks, and each category is described in terms of motivations, capabilities, triggers, methods, and trends. The result is a current and detailed taxonomy usable in planning of digital defense efforts as well as in forensics after an attack has occurred.**

Keywords— **Security, Hacking, Threat Properties, Hacker Taxonomy, Cyber Attacks**

I. Introduction

"*It is said that if you know your enemies and know yourself, you will not be imperiled in a hundred battles; if you do not know your enemies but do know yourself, you will win one and lose one; if you do not know your enemies nor yourself, you will be imperiled in every single battle.*" [1]

As the digital aspect of society and our lives in general becomes ever more important, the defense hereof becomes a higher and higher priority. Billions of dollars are spent each year to protect the systems that form the basis for our online existence against malicious attackers who would steal our data or sabotage our infrastructure, and these spending are rising [2]. It is an uneven battle – attackers need only be successful once while the defenders must be successful every time. Therefore it is imperative to know as much as possible about the would-be attackers to be able to prioritize the defense efforts. This means, that we must be able to gain a better understanding of the different types of hacker attackers, and what kinds of threats they pose.

We want as current and widely accepted terminology as possible to make it possible for users of the taxonomy to search (e.g. on the Internet) for more information on the methods used by and incidents caused by each of the categories. Since the fields of information and network security are fast moving, it is important to be able to keep information current.

Early studies have often been based upon personal observations or on popular media, and until ten years ago only limited research had been done in the field. In 1999 Marcus K. Rogers developed a preliminary taxonomy based on a scientific approach, which has later been expanded and improved by several other authors [3]. In 2006 this work culminated in a division of hackers into 8 categories, and a visualization tool consisting of a two-dimensional circumplex mapping out motivations and competencies of each of these attacker categories. However, just as the Internet as a whole and the ways we use and protect it have developed rapidly and matured over the last years, so has those who would attack it.

In this paper, the categories of hacker attackers are developed to match the current situation (2011/2012) and terminology as well as add entirely new properties to describe them based on threat assessment techniques. This is an important contribution in order to be able to identify potential attackers for a given system, and to take appropriate counter measurements for protection. It also provides valuable input for further research

A. Readers' Guide

This paper is organized as follows: In section II the state of art, specifically the hacker categories described in [4] and the threat properties described in [5], are described. Section III covers the methods used to update the categories, and section IV gives the resulting categories and the characterizing threat properties. Finally, we put our work into perspective in section V and conclude in section VI.

II. State of Art

This section describes the most important state of art and prerequisites.

A. Hacker Categories

In [4] hackers are divided into 9 primary categories, each characterized with distinctive motivation/ competencies profile.

- Novice (NV)
- Cyber-punks (CP)
- Internals (IN)
- Petty Thieves (PT)
- Virus Writers (VW)
- Old Guard hackers (OG)
- Professional Criminals (PC)
- Information Warriors (IW)
- Political Activist (PA)

The characteristics of each group can be plotted into a two-dimensional motivation/skill level circumplex, as illustrated in Fig 1. This visualization tool is designed as an aid in digital forensics to determine which category of hacker might have perpetrated an attack.

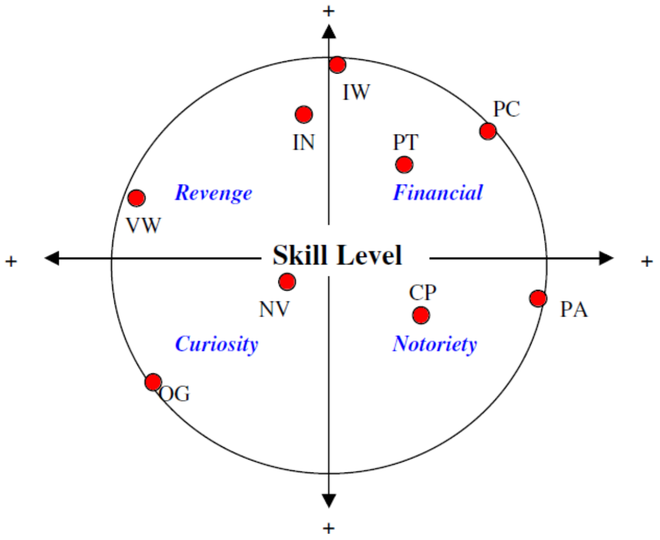

Figure 1 The motivation/skill level circumplex [4].

A. *Threat Properties*

[5] describes a set of threat properties, for use in characterizing a threat to a system. These properties are given in the context of threats to critical infrastructure and are broad enough to encompass accidents and environmental threats as well as attackers:

- Type
- Intent
- Triggers
- Capability
- Methods
- Trends

III. Methods

A combination of several methodologies is used: To update the terminology, we look into the sources where hackers and other denizens of the Internet name themselves and specify their own terminology [6], [7], [8]. This is combined with searches in online security resources [9], [10] to specify the most current names for the hackers contained in each category. The categories are updated – some are combined and a new one is added – based partly on their threat profile and upon recent security incidents.

Each of the new categories is then described using the threat properties presented in [5]. Threat properties are based on the profiles in [4] as well as information extracted from recent incidents and the hackers' own manuals [11], [12].

For this paper, "Intentions" are understood as descriptive of motivation, and for this characterization the four categories used in [4] - Curiosity, Revenge, Financial, and Notoriety - will be used with explanatory comments where needed.

Furthermore, the threat property "Capability", which covers both the skill set and the resources available, is divided into these two separate properties for ease of comparison with the "skill set" property described in [4].

IV. Results

In this section, each of the new categories is described, as well as how the methods were applied: First we develop the categories and the current terminology, the latter to ease information searching on the categories. Then the threat properties of each category are described based on earlier results as well as recent incidents.

A. *Terminology and Categorization*

*1) **Novice:*** According to internet terminology databases [6], [8] the term "novice" applies to someone who is new and not very good at something. In the security community, this category is denominated "Script Kiddies" [9], which in [6] is described as: "n. (Hacker Lingo) One who relies on premade exploit programs and files ("scripts") to conduct his hacking, and refuses to bother to learn how they work." Since this closely mirrors the definition of this category in [4], the name of the Novice category is updated to "**Script Kiddies**"

*2) **Cyber-Punks:*** While the term Cyber-punk is not widely used to describe the kind of hacker, this category describes, there is no other term used in its stead. The Cyber-punks have a threat profile that matches the profile of Virus Writers closely, except the methods of Virus Writers are more specific. While [4] characterize the Virus Writers as mainly revenge-driven, we place their motivations further towards seeking of notoriety based on the research presented in [13]. Therefore, we combine the Virus Writer category into the Cyber Punks category, by adding viruses as a possible method of attack.

*3) **Internals:*** This term is not generally used for this category either; neither in the security community [9], [10], nor in [6] or [8]. However, a very similar term, "Insiders" is widely accepted, and it is used by both the aforementioned sources as well as by security agencies such as the US Secret Service and CERT [14]. Therefore the name of this category will be updated to "Insiders".

*4) **Petty Thieves***: This category very closely resembles its physical-world equivalent except in methods applied, and the term "petty thieves" is well understood in criminal law, and as such, the category name is apt.

*5) **Old Guard Hackers:*** This category is to some extent self-named according to [4]. However, a more widely used term for the same group of people is "**Grey Hat**" as a combination of "White Hat" (beneficent hackers) and "Black Hat" (strictly malicious hackers). [6] defines "Grey Hats" as: "Someone who works on the computer, especially hacking that hacks into systems not to look for anomalies or to destroy a system. They're basically in there screwing around causing minor or no damage." as well as "A grey hat is someone with a mixture of black and white hat experience. Usually, a grey hat is someone who performs network security or system security analysis for organizations." The combination of these two definitions corresponds fairly well with the description given by [4]. The security community does not use either term much, but that may be due to the fact that because the category poses a limited threat, they are not discussed much.

*6) **Professional Criminals:*** The name for this category is widely accepted and also fittingly descriptive.

*7) **Information Warriors***: This category is described as a kind of cyber mercenaries or "hired guns" [4] with a specialty in espionage, most prominently the corporate variety. We consider the financially motivated part of this group to belong in the "Professional Criminals" category, since their threat properties are very much alike. However, the remaining part of this category which is motivated in part ideologically, we would place in a new, emerging category, namely "**Nation States**". Many countries world-wide have in the last few years developed a more or less official offensive capability in the cyber arena. Prominent examples are the US [15] and China [16]. Nation States have been known to conduct operations ranging from industrial espionage [17][18] to sabotage [19] and massive Denial of Service attacks [20] [21]. It remains impossible to prove that operations have been conducted under orders from the actual governments of the nation states, however, the term "Nation States" is still the one that best describes the skills and motivations of this particular category.

*8) **Political Activists:*** In the last year, "Hacktivist" has become a commonly accepted term for this category. Hacktivist groups use the name to describe themselves, and it has been adopted both by the security community [9] and in the popular media.

One special subcategory of political activists, which is not commonly included in this category, is actual terrorist groups such as Al Qaeda or Lashkar-e-Taiba. It is, however, hard to characterize terrorists according to the threat properties, because they actually perform (or potentially perform) three different types of operations: Fundraising, vandalism, and terrorism. While fundraising, they will have a threat profile exactly matching the profile of Petty Thieves [12] employing credit card scams and similar. While doing vandalism, they will act similarly to Cyber-Punks, doing defacements of webpages as well as stealing and publicizing data or minor sabotage. There have been no records of acts of mainly cyber terrorism executed by terrorist groupings, but if and when they occur, we may expect a threat profile similar to Nation States.

This gives the current categories, see Table 1.

TABLE 1. How the new categories corresponds to the ones described in [4].

New Categories	Old Categories
Script Kiddies	Novice
Cyber-Punks	Cyber-Punks, Virus Writers
Insiders	Internals
Petty thieves	Petty Thieves
Grey Hats	Old Guard Hackers
Professional Criminals	Professional Criminals, Information Warriors
Hacktivists	Political Activists
Nation states	N/A, Information Warriors

B. *Threat Properties*

In the following, see Table 2 - 9, each of the categories described above will be characterized according to their threat properties [5].

TABLE 2. Threat properties of the Script Kiddies category.

Type	**Script Kiddies (SK)**
Intent	Curiosity, Notoriety.
Triggers	This group does not need any special triggers to execute an attack. Targets are typically chosen at random.
Capability - Skills	Very low.
Capability - Resources	Very low - Script Kiddies typically work alone and are not dedicated enough to their hacking to have particularly strong or specialized equipment.
Methods	Tools and scripts downloaded for free from the Internet. The tools scan random IP blocks on the Internet for weaknesses and allow the Script Kiddies to exploit them as they are found [22].
Trends	There is more and more money in cyber crime, so even of the amount of tools and scripts available on the Internet for free is ever increasing, the truly disruptive and effective crimeware is only available for money. Therefore, while Script Kiddies can still do a lot of damage to systems with no or low security [23], they are unlikely to do any serious damage to well-protected systems.

TABLE 3. Threat properties of the Cyber-Punks category.

Type	**Cyber-Punks (CP)**
Intent	Notoriety (with the occasional financial or vindictive intent).
Triggers	This group does not need any special triggers to execute an attack, however higher profile targets (e.g. military or government targets) are more likely to attract attention from Cyber-Punks.
Capability - Skills	Medium skill level. Typically a generalist level of knowledge in both software and hardware as well as programming skills.
Capability - Resources	Cyber-Punks may have acquired some inexpensive specialized equipment, and may partake in information sharing in specialized hacking forums on the Internet or be members of hacking groups.
Methods	Cyber-punks may use tools downloaded from the Internet which they modify to suit their purpose. For financial support, some are engaged in credit card number theft and telecommunications fraud. [4]

Trends	The fame and notoriety of successful cyber-punks like Kevin Mitnick and more recently George Hotz (a.k.a. GeoHot) is the hacker equivalent to the American Dream. When popular media shows a hacker attention, or even when popular hacker movies premiere in the cinemas, there is a surge in the activity of Cyber-Punks [24].

TABLE 4. THREAT PROPERTIES OF THE INSIDERS CATEGORY.

Type	**Insiders (I)**
Intent	Revenge, Financial.
Triggers	Negative work-related event [14]. The target of an Insider attack is usually the workplace or former workplace of the attacker.
Capability - Skills	Since Insiders per definition are attacking systems they have inside information about and usually extensive specialized knowledge of, their attack skills should be considered high.
Capability - Resources	While Insiders usually work alone, they have physical and privileged digital access to the system, and for an attack that amounts to a considerable resource.
Methods	Insiders have three main avenues of attack: Sabotage, theft of intellectual property, and fraud. In all of these attacks, the Insider abuses his or her position of trust to commit the attack.
Trends	The amount of Insider attacks compared to incidents performed by outsiders is in decline. According to [25] 21% of attacks are caused by Insiders. About one third of the respondents viewed the Insider attacks to be more costly than outsider breach, compared to 25% in 2010. 22% of the Insider attacks were executed using hacker scripts and tools.

TABLE 5. THREAT PROPERTIES OF THE PETTY THIEVES CATEGORY.

Type	**Petty Thieves (PT)**
Intent	Financial.
Triggers	This group does not need any special triggers to execute an attack.
Capability - Skills	Medium skills. The Petty Thieves typically move into the cyber domain since their traditional targets move there. They learn the specific skills needed to execute their attacks successfully, but they do not have any interest in the technology in and of itself.
Capability - Resources	Petty Thieves are usually not interested in gaining notoriety - on the contrary since that may prove detrimental to their work [4], so they are usually not active members of hacking communities. Since they resort to petty theft, they are not expected to have many monetary resources available, however they may have specialized equipment necessary to work their trade.
Methods	Spam, credit card scams, identity theft, using crimeware or homemade scripts and tools.
Trends	Petty theft is still very much alive on the Internet [12], and the attack vectors have not changed radically over the last few years. It has become more accessible for the non-technical Petty Thief, though, with the introduction of professional easy-to-use crimeware availability.

TABLE 6. THREAT PROPERTIES OF THE GREY HATS CATEGORY.

Type	**Grey Hats (GH)**
Intent	Curiosity, Notoriety.
Triggers	This group does not need a special trigger, however they are attracted to high-security targets. They prefer targets they consider challenging to attack or which they perceive contain information they are interested in obtaining, which may be sensitive in nature.
Capability - Skills	High skills, often including very specialized skills within computer and network security.
Capability - Resources	While Grey Hats tend to work alone, they also typically engage in heavy knowledge exchange and build upon the equally specialized tools of their peers [4].
Methods	Grey Hats may exploit more or less known vulnerabilities or even develop new 0-day attacks to gain access to their target systems. Usually they will do little or no damage to the system, even though they may steal and publicize choice bits of data and information.
Trends	While this category of hackers usually do not do major damage, the recent example of the Wikileaks whistleblower, Bradley Manning, proves, that this is not always the case [26].

TABLE 7. THREAT PROPERTIES OF THE PROFESSIONAL CRIMINALS CATEGORY.

Type	**Professional Criminals (PC)**
Intent	Financial.
Triggers	No triggers needed. Professional Criminals are just that - professional. They analyze rewards versus risks before they attack, and they are not expected to attack targets without a viable business case.
Capability - Skills	Very high, including specialized skills within computer security, crimeware, and the sectors of society where they do their business.
Capability - Resources	The Professional Criminals work together in an organized fashion mimicking legitimate business. This includes structured enterprises and supply chains with each part of the chain having whatever specialized skills and equipment needed. They can be expected to have access to large amounts of money and be willing to invest them if the business case is sound.
Methods	Professional Criminals employ a plethora of methods, and they develop continually. Favoured attack vectors are phishing, spam, botnets, Man-in-the-Browser and keyloggers.
Trends	The use of botnets to steal financial information (e.g. credit card numbers or online

	banking details) is on the rise [27] as well as corporate espionage and identity theft [28]. Likewise, the Professional Criminals are exploring new attack vectors by targeting mobile devices [29] and using cloud technology to perform their illegal activities.

TABLE 8. THREAT PROPERTIES OF THE HACKTIVISTS CATEGORY.

Type	Hacktivists (H)
Intent	Notoriety, Revenge. Hacktivist groups are per definition ideologically motivated, though some groups lean heavily towards being motivated by the fame. This is especially true for some of the newer, high-profile groups, who admit to "doing it for the lulz". [30] suggests that their motivation may be similar to that of the character "The Joker" in the Batman movie "The Dark Knight" - they simply enjoy watching the world burn.
Triggers	Any real or perceived insult to their ideology.
Capability - Skills	While the skill levels of Hacktivist groups vary widely, they tend to have a number of core members with high technical skills. Some Hacktivist groups, most famously "Anonymous", arrange hacking schools for their newer members to increase the level of skill among them [11].
Capability - Resources	While the monetary resources may be limited, some Hacktivist groups have a huge amount of members and followers. They can be expected to have access to much specialized and even potentially sensitive or restricted information [insider threat study] as well as the manpower to execute devastating DDoS attacks using only volunteer participants. Lately this includes physical-world participation as well.
Methods	Hacktivists favour exploiting common (known) vulnerabilities (e.g. SQL Injection or Buffer Overflow vulnerabilities) to gain access to sensitive data which are then publicized. [31], [32]. Another preferred method is (D)DoS attacks [33], [34].
Trends	Hacktivism becomes more and more mainstream [35] but wanders on the knife's edge between civil disobedience and outright terrorism. Recently, it has gained new legitimacy in the western world by being combined with legal demonstrations such as "Occupy Wall Street" - in e.g. China, nationalistic hackers have been celebrated by the general populace for years [36].

TABLE 9. THREAT PROPERTIES OF THE NATION STATES CATEGORY.

Type	Nation States (NS)
Intent or motivation	Revenge, Financial. The former is in this context understood as a general term for aggression. The Nation State in question may be aggressor.
Triggers	Typically, Nation States attacks are triggered by geo-political conflict.
Capability - Skills	Nation States may have access to the competencies and the knowledge of an entire nation. Even if this may be a truth with modifications, Nation State actors can always be considered to have very high skills.
Capability - Resources	A Nation State typically have access to more funds, better equipment, and more thorough intelligence than any other group of attackers. Their resources are vast.
Methods	While Nation States behave differently and often act very covertly on the Internet, there are a few common characteristics. First of all, they target resources of national impact, e.g. critical infrastructure [17], [18]. Methodologies vary, but they often combine social engineering techniques and spear-phishing with more or less sophisticated trojans [18], [19].
Trends	Nation States are becoming more prominent on the Internet with many countries establishing cyber commands [15], [16]. Aggression levels are high, especially between the East, led by China, and the West, led by the US - there have even been talk of new Cold War in the cyber domain [37], [38].

The circumplex developed in [4] and described in section II only illustrates two of the threat properties (Intent and Capability – Skills), but it can still be a help to get an updated overview of the categories, see Fig. 2.

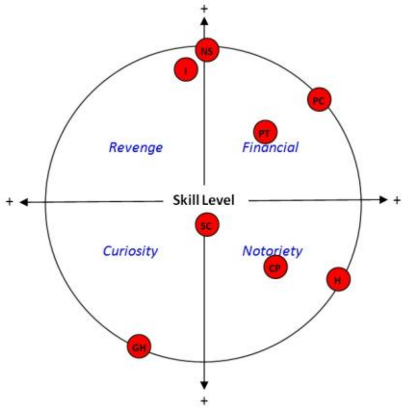

Figure 2 Circumplex illustrating the new categories**.**

Comparing Fig. 1 and Fig. 2, it is apparent that the threat profiles are coming together in the right hand side of the diagram, showing that financial and notoriety aspects are increasingly important motivations for most of the attackers. This coincides well with the notion that the hackers are getting more organized and have an increasingly professional approach to their criminal activities.

This is of course only a general picture, and it does not mean that attackers motivated by curiosity or revenge does not exist or can be ignored.

V. Discussion

This updated taxonomy is created for use in prioritizing digital defense efforts as well as in forensic investigations after an attack has occurred. For the former, an organization must create a target profile – which motivation would an attacker have to attack a specific system? Which level of skill is needed to penetrate the defenses? The defense planner can then use the taxonomy to determine which categories of hackers are most likely to attack the system, and then prioritize defense against the methods utilized by these categories, while keeping an eye on relevant triggers.

For forensic aid, the incident responder can look into the methods, presumed motivations, and demonstrated level of skill to get a clearer understanding of, which category the attacker may belong to.

For lack of space, we will not go into details about the verification of this taxonomy. Suffice to say, it must be verified by applying it to a significant number of security incidents where the perpetrator has been or can be identified.

VI. Conclusion

The Internet underground has evolved and matured much these last few years, and the characteristics of hackers and hacker groupings have changed as well as the terminology used to describe them.

We have developed an updated taxonomy for understanding and describing hackers in digital defense planning and forensics. Hackers are divided into categories, each labelled according to the current terminology in the hacker and security communities, and for each category the threat properties: Intent, capability, triggers, methods, and trends are mapped.

References

[1] Sun Tzu, *Art of War*, China, ca. 500 B.C.

[2] J. Penn, *Security Futures - Selected results from our Forrsights Security Survey, Q3 2010*, Forrester Research, Sept. 23, 2010.

[3] C. S. Fötinger, and W. Ziegler, "Understanding a hacker's mind – A psychological insight into the hijacking of identities" Danube-University Krems, Austria, 2004.

[4] M. K. Rogers, "A two-dimensional circumplex approach to the development of a hacker taxonomy," *Digital Investigation*, vol. 3, pp. 97 – 102, 2006.

[5] J. Moteff, "Risk Management and Critical Infrastructure - Protection: Assessing, Integrating, and Managing Threats, Vulnerabilities and Consequences," Congressional Research Service, The Library of Congress, Washington, USA, 2005.

[6] (2011) The Urban Dictionary website. [Online]. Available: http://www.urbandictionary.com/

[7] (2011) sla.ckers website [Online]. Available: http://sla.ckers.org/

[8] (2011) Wikipedia website [Online]. Available: http://en.wikipedia.org/

[9] (2011) InfoSec Island website [Online]. Available: http://www.infosecisland.com/

[10] (2011) Securityweek website [Online]. Available: http://www.securityweek.com/

[11] Denizen, cred, et al., "The #OpNewblood Super Secret Security Handbook," Anonymous, 2011.

[12] E.J. Hilbert II, "Hacking for Profit: Credit Card Fraud - A Beginners Guide," Federal Bureau of Investigation, Los Angeles, USA, 2004.

[13] S. Gordon, "The Generic Virus Writer II", *6th International Virus Bulletin Conference*, Brighton, UK, September 1996

[14] M. Keeney, D. Cappelli, et al., "Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors" U.S Secret Service and CERT, USA, 2005

[15] *U.S. Cyber Command Fact Sheet*, US Department of Defense, May 25, 2010.

[16] W. Hagestad II, "China: A Comparative Analysis of Government & Nationalistic Threat Vectors", Red Dragon Rising, USA, 2011

[17] (2011) Sophos: Operation Aurora website [Online], Available: http://www.sophos.com/en-us/security-news-trends/security-trends/operation-aurora.aspx

[18] *Global Energy Cyberattacks:"Night Dragon"*, McAfee Foundstone Professional Services and McAfee Labs, Feb. 10, 2011

[19] N. Falliere, L. O. Murchu, and E. Chien, "W32.Stuxnet Dossier", Symantec Security Response, Feb. 2011

[20] (2011) Arbor Networks – Security to the Core website [Online], Available: http://asert.arbornetworks.com/2008/08/georgia-ddos-attacks-a-quick-summary-of-observations/

[21] *Ten Days of Rain - Expert analysis of distributed denial-of-service attacks targeting South Korea*, McAfee, 2011

[22] L. Spitzner, "The Tools and Methodologies of the Script Kiddie - Know Your Enemy", USA, 2000.

[23] (2011) The Conversation website [Online], Available: http://theconversation.edu.au/unijobs-com-au-website-hacked-more-than-600-passwords-exposed-3759

[24] (2011) InfoSec Island: The Top Three Hacker Movies Of All Time website [Online], Available: https://www.infosecisland.com/blogview/16293-The-Top-Three-Hacker-Movies-Of-All-Time.html

[25] *2011 Cybersecurity Watch Survey: Organizations Need More Skilled Cyber Professionals to Stay Secure*, CSO, Secret Service, Cert, an Deloitte, Jan. 31, 2011

[26] (2011) International Business Times: Who is Bradley Manning website [Online], Available: http://www.ibtimes.com/articles/86525/20101129/us-wikileaks-bradley-manning-factfile-who-is.htm

[27] *Botnets: The New Threat Landscape*, Cisco, 2007.

[28] (2011) eWeek.com: Sony PlayStation Network Data Breach Compromises 77 Million User Accounts [Online], Available: http://www.eweek.com/c/a/Security/Sony-PlayStation-Network-Data-Breach-Compromises-77-Million-User-Accounts-208028/

[29] (2011) eWeek.com: Zeus Trojan Variant Found on BlackBerry Phones [Online], Available: http://www.eweek.com/c/a/Security/Zeus-Trojan-Variant-Found-on-BlackBerry-Phones-422999/

[30] (2011) Krypt3ia: Virtual Arkham: Explaining Anonymous, Lulzsec, and Antisec Animus in Our Digital Gotham City [Online], Available: http://krypt3ia.wordpress.com/2011/08/19/virtual-arkham-explaining-anonymous-lulzsec-and-antisec-animus-in-our-digital-gotham-city/

[31] (2011) The Tech Herald website [Online], Available: http://www.thetechherald.com/article.php/201122/7230/LulzSec-Sony-was-asking-for-it-millions-of-records-compromised-Update-2

[32] (2011) Tech News World website [Online], Available: http://www.technewsworld.com/story/72924.html

[33] (2011) Sophos: Naked Security website [Online], Available: http://nakedsecurity.sophos.com/2011/01/26/egypt-versus-the-internet-anonymous-hackers-launch-ddos-attack/

[34] (2011) The New Internet: Hacktivist 'the Jester' Takes Credit for WikiLeaks DoS Attack [Online], Available: http://www.thenewnewinternet.com/2010/11/29/hacktivist-the-jester-takes-credit-of-wikileaks-dos-attack/

[35] (2011) The Guardian - Anonymous: peering behind the mask [Online], Available: http://www.guardian.co.uk/technology/2011/may/11/anonymous-behind-the-mask

[36] (2011) Popsci: The China Syndrome website [Online], Available: http://www.popsci.com/scitech/article/2009-04/hackers-china-syndrome

[37] (2011) ZDNet: Welcome to the New Cold War [Online], Available: http://www.zdnet.com/blog/government/welcome-to-the-new-cold-war-china-vs-the-united-states/10289

[38] (2011)The New Internet: McAfee CSO Predicts New Cold War in Cyber Domain [Online], Available: http://www.thenewnewinternet.com/2011/06/16/mcafee-cso-predicts-new-cold-war-in-cyber-domain-hackers-for-hire/