J Comput Virol
DOI 10.1007/s11416-006-0015-z

ORIGINAL PAPER

On the definition and classification of cybercrime

Sarah Gordon · Richard Ford

Received: 13 January 2006 / Revised: 11 February 2006 / Accepted: 29 March 2006

Abstract The idea of Cybercrime is not new, yet there is significant confusion amongst academics, computer security experts and users as to the extent of real Cybercrime. In this paper, we explore the breadth of computer-based crime, providing a definition of the emerging terms "Cybercrime" and "crimeware". We then divide Cybercrime into two distinct categories: Type I Cybercrime, which is mostly technological in nature, and Type II Cybercrime, which has a more pronounced human element. We then use two case studies to illustrate the role of crimeware in different types of Cybercrime, and offer some observations on the role of cognition in the process of Cybercrime. Finally we provide several suggestions for future work in the area of Cybercrime.

1 Introduction

Discussions of Cybercrime can be found in diverse sources including academic journals, generalist computer magazines, newspaper articles and online; it has been the subject of movies, television programs and radio broadcasts. However, despite an apparent acceptance of and familiarity with the term, there exist dramatically varied views of what Cybercrime *is*. This lack of definitional clarity is problematic as it impacts every facet of prevention and remediation. In addition, research shows that the number of people and businesses impacted by various types of perceived cybercrime is growing with no signs of declining [2,12,21].

In this paper we examine various dimensions of Cybercrime; after examining some of these definitions, we offer a more inclusive definition before delineating these crimes into two subtypes. Further, we define the term "crimeware", now in common usage but with varied and often context-based definition, and illustrate this definition's breadth of similarities and differences with existing usages. Finally two case studies are provided, illustrating the varying effects of education and perception with respect to Cybercrime on home users.

2 Definitions

Despite the fact that the word "Cybercrime" has entered into common usage, many people would find it hard to define the term precisely. Furthermore, there is no catch-all term for the tools and software which are used in the commission of certain online crimes. In the next two sections, we will attempt to rigorously define Cybercrime and formalize an emerging term, crimeware, which is an inclusive term for the many different Trojans, Viruses, Bots, Spyware and Worms which are instrumental in facilitating certain Cybercrimes.

2.1 Cybercrime

Like traditional crime, Cybercrime has many different facets and occurs in a wide variety of scenarios and environments. Current definitions of Cybercrime have evolved experientially. They differ depending on the

S. Gordon (✉)
Symantec Security Response, 2500 Broadway,
Santa Monica, CA 90494, USA
e-mail: sarah.gordon@symantec.com

R. Ford
Department of Computer Sciences, Florida Tech.,
150 W. University Blvd, Melbourne, FL 32901, USA
e-mail: richard.ford@fit.edu

perception of both observer/protector and victim, and are partly a function of computer-related crimes geographic evolution. For example, The Council of Europe's Cybercrime Treaty uses the term "Cybercrime" to refer to offences ranging from criminal activity against data to content and copyright infringement [13]. However, Zeviar-Geese [22] suggest that the definition is broader, including activities such as fraud, unauthorized access, child pornography, and cyberstalking. The United Nations Manual on the Prevention and Control of Computer Related Crime includes fraud, forgery, and unauthorized access [19] in its cybercrime definition.

As you can see from these three definitions, Cybercrime can occur across a broad spectrum. In many ways, our argument regarding Cybercrime is similar to our previous argument concerning the utility of the word "cyberterrorism" [8]. In the case of cyberterrorism it is our belief that the term itself is misleading in that it tends to create a vertical representation of a problem that is inherently horizontal in nature. Similarly, a criminal will not care whether a crime is "cyber" in nature or not; instead, all methods available will be exploited.

Given this position, we believe there are significant benefits to deleting the word from the lexicon entirely! However, given that this is not likely to occur, the next best thing is to attempt to define the word as meaningfully as possible. Unfortunately, modelling cybercrime definition upon existing categories in work such as Parker [16] is problematic as existing work tends to be descriptive rather than based upon a theoretical framework. With this in mind, we define Cybercrime as: "any crime that is facilitated or committed using a computer, network, or hardware device".

The computer or device may be the agent of the crime, the facilitator of the crime, or the target of the crime; indeed, the crime can take place on the computer alone, or in other non-virtual locations. Given the breadth of this definition it is beneficial to subdivide cybercrime into two distinct types; thus we define operationally for the purpose of this research Type I and Type II Cybercrime. An additional advantage of this approach is that it is easy for researchers to define the topic too narrowly. By explicitly highlighting these two facets of Cybercrime, we hope to provide additional emphasis on the breadth of the issue.

Further, our goal is not to legally define Cybercrime – such a definition is beyond the scope of this paper. Instead, we attempt to create a conceptual framework which lawmakers can use in order to create legal definitions which are meaningful from a technical and societal perspective. We recognize that current legal definitions of Cybercrime vary drastically between jurisdictions; however, if technicians in the field worldwide can adequately grasp the nuances of electronic crime, more cohesive legal definitions may result.

Under our proposed scheme, Type I cybercrime has the following characteristics:

1. It is generally a singular, or discrete, event from the perspective of the victim.
2. It often is facilitated by the introduction of crimeware programs such as keystroke loggers, viruses, rootkits or Trojan horses into the user's computer system
3. The introductions can, but may not necessarily be, facilitated by vulnerabilities.

A single event or discrete instance, from the user's perspective, might look something like this:

1. The user goes online to perform a task, i.e. access the WWW, or read/reply to e-mail.
2. User takes action which then allows the criminal access to information (entering personal information on the look-a-like site, (or) clicks on some object resulting in the download of a Trojan or keystroke logger.
3. This information is used by the attacker.
4. The user becomes aware of the crime – this is the single event from the perspective of the user. This usually occurs much later in the lifecycle of the Cybercrime.
5. The crime is investigated and resolved.

This type of Cybercrime requires that data be protected from traditional threats such as viruses and worms, but also that users be cognizant of the concept of "vulnerabilities". This is a huge "thought change" required in the user population.

Vulnerabilities are often found in COTS software; for example, in 2005, Microsoft documented several key vulnerabilities in its popular Internet Explorer application. Criminals controlling a web site may use computer code capable of exploiting such a vulnerability in a Web Browser to place a back-door program on the computer of a visiting user.

Examples of this type of cybercrime include but are not limited to phishing attempts, theft or manipulation of data or services via hacking or viruses, identity theft, and bank or e-commerce fraud based upon stolen credentials.

Type II cybercrime, at the other end of the spectrum, includes, but is not limited to activities such as cyberstalking and harassment, child predation, extortion, blackmail, stock market manipulation, complex corporate espionage, and planning or carrying out terrorist activities online. The characteristics of Type II cybercrime are that:

1. It is generally facilitated by programs that do not fit under the classification crimeware. For example, conversations may take place using IM (Instant Messaging) clients or files may be transferred using the FTP protocol.
2. There are generally repeated contacts or events from the perspective of the user.[1]

A series of events in the lifecycle of a Type II Cybercrime might look something like this:

1. User(a) goes online to see what she can find out about llama farming.
2. User(a) decides to participate in on-line forum about llama farming.
3. User(b) sees User(a), watches her participation in the forum for several days, responds to some of her comments.
4. User(b) then sends a request for private chats using a common Instant Messaging client.
5. User(a), being familiar with User(b) via the on-line forum, responds positively and they begin to chat daily as well as participate in the Forum. This is a period known as instilling trust.
6. After several interactions User(a) reveals that she is single, likes llamas, has a quarter of a million dollars available to start a llama farm, and that she likes to go to concerts. She tells him her real name is Jenny.
7. User(b) asks User(a) to meet in person and go to a concert.
8. User(a) becomes suspicious when User(b) will not give his contact information other than on-line information, and she refuses.
9. User(b) becomes irrational and begins to post false claims against User(a) in the on-line forum, accusing her of fraud, and of being there to pick up men, not to find others interested in llamas. He posts her home number. He also goes onto other forums posing as User(a), and leaves messages asking for dates – leaving her real phone number and real name.
10. User(a) tries to defend herself in the Forum, and asks User(b) privately to stop, using IM. She begins to get numerous e-mails about the dates she requested – and realises then that someone is impersonating her online. She confronts User(b) with her suspicions.
11. User(b) becomes more irrational and begins to make hang-up and harassing phone calls to User(a). User(a) becomes afraid for her safety.
12. The telephone company and the local police become involved.
13. User(a) files charges against User(b), who is, it is later learned, a former child-pornographer with links to organized crime, under investigation for the disappearance of three women he allegedly met on the Internet.

While such an exchange may seem far-fetched, cyberstalking is a very real problem in today's online community [1]. As such, it clearly is related to – but different from – Type I Cybercrimes which are more technical in nature.

Understanding Cyberstalking's role in our cybercrime classification is important, as it illustrates the utility of the scheme. Consider, for example, the case of Amy Boyer, who was murdered after being stalked online. The perpetrator ultimately used several online tools and websites to harass his victim, culminating in Boyer's murder on October 15, 1999. While some have questioned whether this was a genuine computer crime (for a good discussion of this issue and an overview of this and other similar cases, see [9], our belief is that such crimes are by necessity a form of Cybercrime, as the computing element fundamentally changes the scope of the crime. However, the cyber element of the crime can be quite weak.

Thus, Cybercrime really presents a continuum ranging from crime which is almost entirely technological in nature and crime which is really, at its core, entirely people-related (see Fig. 1). Consider, for example, a fraud carried out via e-mail where the user is directly and simply asked to send money to a particular physical address in return for some service which never materializes. At its core, this fraud would work via regular paper mail or telephone. As such, it is really not a technolog-

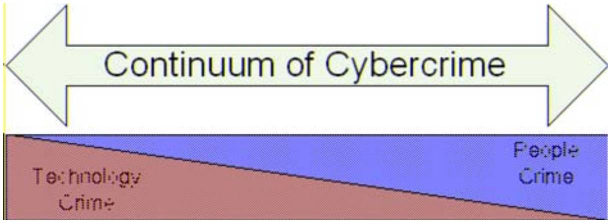

Fig. 1 The Continuum of Cybercrime. Areas defined as Cybercrime are very broad in nature – some crimes have only a peripheral cyber element, whereas others exist only in the virtual world

[1] One clarifying point is needed. In cases of cyberstalking (see, for example, the case of Amy Boyer discussed elsewhere in this paper) the victim may not be aware of the underlying events. However, the causal events were ongoing – that is, there is not one single event as it pertains to the victim.

Table 1 Cybercrime by type

Examples of different cybercrime by type, examining the software used in each case

Example	Type	Software	Crimeware
Phishing	I	Mail client	No
Identity Theft	I	Keylogger, Trojan	Yes
Cyberstalking	II	Email Client, Messenger Clients	No
DDoS	I	Bots	Yes
Cyberterrorism (communication)	II	Steganography, Encryption, Chat Software	No

ical issue, though the perpetrator can (and frequently does) use certain attributes of technology to his or her advantage. At the other end of the scale, the user whose machine is penetrated but suffers no financial loss has not really participated in the Cybercrime – the crime is purely technological in nature.

Similarly, there are likely to be very few events which are *purely* Type I or Type II; these types represent either end of a continuum. The important fact is to recognize the breadth of the scale; it is all too easy to ignore the end of the scale which one is least accustomed to. For example, a traditional investigator may be more capable of investigating crimes that are more people-centric than technological; similarly, computer security experts are more likely to focus their efforts on issues they see as technological, when simple technological countermeasures could provide significant protection from more people-centric crimes.

Another important aspect to consider is the cost-benefit issue for the cybercriminal. As pointed out in Kshetri [14], the motivators can be either financial, psychological, or a combination of the two. Offsetting this are the expectation of a penalty (that is, the likelihood and consequences of getting caught) and the financial return. This fits our model well in that it treats Cybercrime very broadly, and includes crimes that have no financial motivation.

2.2 Crimeware

The software used in Cybercrime is sometimes referred to as crimeware (see, for example, [20] for a common usage definition). We define crimeware as software that is:

1. used (directly or indirectly) in the commission of the criminal act;
2. and not generally regarded as a desirable software application from the perspective of the computer user;
3. and not involuntarily enabling the crime.

The reasoning behind this definition is that it explicitly excludes legitimate programs which may be leveraged by an attacker. For example, a browser which has a vulnerability in it is not meaningfully crimeware – it is simply flawed software. In addition, note that *the type of crime carried out is not specified.* This is an important distinction from other definitions of crimeware, which frequently limit crimeware's scope to just that software used for financial crime. This is an artificial distinction, as it defines a program based upon how it is used, not on its content. These issues are further discussed below.

Like Cybercrime itself, the term crimeware covers a broad spectrum. However, it is important to remember that not all software used in the commission of a computer-based or computer-facilitated crime can be legitimately termed crimeware. For example, while an IM client may be used in the commission of a Cybercrime, the IM application software itself is not considered crimeware. FTP clients may be used in the commission of crimes; however, they are not considered crimeware. Crimeware does, however, include programs which may be classified as bots, keystroke loggers, spyware, backdoors and Trojan horses. Additionally, some cybercrime may involve both crimeware and legitimate programs.

The classification of crimeware is important in that it effects the evaluation of security software. If, for example, we classify software contextually – that is, depending on its *role* – the identification of software is essentially undecidable; detection is entirely arbitrary, making certification and measurement of efficacy impossible.

Our definition is not simply based upon the niceties of evaluation, however. Classifying software contextually makes little sense in terms of risk management. Consider the Instant Messaging example from above. Instead of simply classifying the IM client as "bad" it is better to recognize that it introduces a particular risk into the environment. This risk may or not be acceptable; it does not mean that IM clients are undesirable – just that the changes they introduce to the environment should be managed (Table 1).

3 Case study: Type I cybercrime

Kobe,[2] a middle school instructor, recently fell victim to a phishing attack. He was using e-Bay to sell one of

[2] Names and places in this section have been changed in order to respect the privacy of the individuals involved.

his vehicles, and he found a suitable buyer within several days. The buyer paid for the vehicle, Kobe received payment and removed the listing from e-Bay.

He was somewhat puzzled when he logged into his e-Bay account and was informed he had "one item for sale." He looked at the page, and sure enough, there was the vehicle – the same one he had just sold – for sale. Then he noticed something else wrong – very wrong. The e-mail address that was listed for his contact information was not his. It was very similar, so much so that most people would not notice the change. Kobe e-mailed the "seller" and offered to buy the vehicle, just to see what the response would be. The "seller" thought Kobe was just another buyer, and when Kobe offered to buy the vehicle, the seller made arrangements for the money to be sent. As it turned out, the "seller" was located in Chicago. Kobe gave the FBI the information, and they tracked down the fraudsters.

How did the fraudsters gain access to Kobe's account in the first place? A phishing e-mail stating his account had been compromised asked him to click on a URL to go to his e-Bay account and validate his ID. He clicked on the URL and was taken to a page that looked identical to his e-Bay login page, and he was asked to type in his account information. The criminals used that information to log into his legitimate account and change the contact phone number.

The software used to commit and enable this crime consists of both non-crimeware and crimeware. The non-crimeware programs are those which are used daily by many people in the course of doing business on the Internet: e-mail and a browser. The crimeware program used in this case was executable code that took Kobe to the look-a-like WWW site. The result of the use of the crimeware was the obtaining of Kobe's confidential information, and the resultant placement of a "copycat" for sale ad, designed to lure users into repeatedly purchasing non-existent goods. While the criminals attacked many people using the look-a-like site phishing scam, from the perspective of each user, this crime was a "one time event"[3]. And, while from the perspective of e-Bay, the cybercrime represented multiple frauds, from the perspective of the other victims – those who sent money to the fraudsters, this was also a one-time event.

4 Case study: Type II cybercrime

In some cases, determining whether or not actions are "cybercrime" requires determining if the actions are objectionable. This can depend on the cognitions of the potential victim, or may be clearly recognized according to law or statute.

Consider the case of Roger and Hannah. Several months after the end of their relationship Roger received an e-mail from Hannah. It seemed to be harmless, stating simply that she had been thinking about him and missed him. Roger did not respond to the e-mail, as he did not wish to appear interested in resuming the relationship. Over the next several months, Hannah continued to e-mail Roger from time to time, saying that she knew she should leave him alone, but couldn't. Initially, Roger was not too concerned about Hannah's behaviour; however, when the e-mails persisted the entire year, he became concerned and sent Hannah a strongly worded e-mail telling her he did not want any further contact with her, and after an initial refusal to comply, Hannah did stop all contact.

4.1 Discussion

The definition of Cybercrime and the differentiation of types of Cybercrime are extremely important for several reasons. Definitions provide researchers with a common language, necessary for sound collaboration (or even meaningful discussion). Furthermore, definitions help determine the scope of the problem to be addressed, and are necessary for clear communication about a subject. The lack of clear definitions is exemplar of immature and unscientific approach to the problem. This is not surprising, given the relative immaturity of the security and in particular antivirus industries [6,15].

Unfortunately, the definitions of crimeware currently in use by both generalist and specialist populations adds to the confusion by failing to delineate correctly between legitimate software which is used to facilitate a crime and by software whose primary purpose is to execute a crime. It is worth noting at this juncture that software does not have "intent"; instead, we can only attempt to make a best guess as to the intent of the programmer of the software [7]. Consider these two definitions:

(a1) Software designed to steal personal information or perform some other illegal operation. It is malicious software that causes a crime to be committed. See warez and malware.

(a2) Software that helps someone perform an unwanted or illegal act via the computer. Programs and documentation that enable less technical people to set up their own spam, virus or phishing attacks are crimeware, essentially a software development kit for scoundrels. The good news is that the documentation is

[3] A user may receive many "individual event" e-mails – but each is considered a discrete event.

probably as horrid as that of most popular commercial software [17].

And:

[b] Crimeware is a relatively new term that is used to describe software used to commit crime [11].

We have already shown that software that helps people to perform an illegal act via the computer is not necessarily bad. The claim that software defined as crimeware *causes* a crime to be committed is unsupported; clearly, it is the cybercriminal who makes the decision to commit the crime. However, it is the opening sentence of a2 that is more cause for concern, stating "software that helps someone perform" a crime. Definition [b] is problematic in that there are many types of software used to commit crime, as demonstrated by our Case Studies, and considering all of these programs "crimeware" would be inappropriate and counterproductive – essentially classifying almost any program as crimeware under certain circumstances. Thus, these types of definitions are of limited use as they tend to unrealistically broaden the range of programs that could operationally be considered crimeware, robbing the term of meaning.

Another type of definition, from Davis et al. [3] refers to another type of software to help define Crimeware, stating "Crimeware is similar to spyware in that it monitors a user's online behaviour; however, crimeware programs have been modified for the purpose of stealing a user's personal information." This type of overgeneralization tends to limit the scope of the problem in that it considers only monitoring programs to be crimeware, and perhaps more problematically, it does not differentiate between programs that monitor legitimately versus those that monitor illegitimately.

At the very opposite end of this spectrum [18] limits crimeware to those programs used to commit financial crime, as opposed to other types of malware which may not aid in financial crime. "Crimeware is a term coined by Peter Cassidy, Secretary General of the Anti-Phishing Working Group, to distinguish computer programs (and coordinated, interlocking sets of programs) that are designed specifically to animate financial crime from other kinds of malevolent code packages." This narrow definition limits the scope of the problem artificially, it does not even address the issue of programs which are shown to be behaviourally malware (such as a program designed to exploit a vulnerability and obtain root access remotely) and which *could* be used to commit financial or other cybercrime; rather, it excludes them!

In light of the issues introduced by the current span of operational definitions of "crimeware," we consider first the Case Study of Roger and Hannah detailed in the previous section. Zona et al. [23,24] describe a typology of cyberstalking based on the relationship between the victim and offender that is consistent with the case of Roger and Hannah. Classified as "Simple Obsessional", such cases "typically involve a victim and a perpetrator who have a prior relationship. This group comprises the largest of the categories (47 %), and also poses most threat to the victim. The motivation behind this may be coercion to re-enter a relationship, or revenge aimed at making the life of the former intimate uncomfortable through the inducement of fear."

Additionally, this type of behaviour has the potential to develop into something far more serious. According to the [4] "while some conduct involving annoying or menacing behaviour might fall short of illegal stalking, such behaviour may be a prelude to stalking and violence and should be treated seriously." Helpguide [10] concurs: "Stalking is unpredictable and should always be considered dangerous."

Indeed, the question of whether or not unwanted (but otherwise benign) e-mail constitutes stalking is addressed clearly by ([5]; see also the following statues: Michigan, (MSA Sect. 28.643(8)E,vi) , Oklahoma, (21 Okl. St.Sect. 1173, F 4f), Alaska (AK St. 11.41.270)), all of which place "unwanted e-mail contact" into the category of cyberstalking. Roger did not consider Hannah's actions "cyberstalking"; however, the question remains, at what point does "unwanted contact" constitute "cyberstalking" or harassment? In any case, the resolution of situations involving unwanted contact is sometimes not benign; as evidenced by the following examples:

A San Diego college student's actions reported in [4]: An honours student from the University of San Diego terrorized five female university students over the Internet for more than a year. The victims received hundreds of violent and threatening e-mails, sometimes receiving four or five messages a day. The graduate student, who has entered a guilty plea and faces up to 6 years in prison, told police he committed the crimes because he thought the women were laughing at him and causing others to ridicule him. In fact, the victims had never met him."

While Cybercrime is only now gaining high visibility, these cases are not exceptions. There have been cases of the Internet being used to facilitate crime throughout the past decade. For example, in 1999, a 50-year-old man who had used the Internet to solicit the rape of a woman who had rejected his romantic advance pled guilty to one count of stalking and six counts of soliciting sexual assault. His actions included impersonating his 28-year-old victim in various Internet chat rooms and online bulletin boards, posting messages allegedly from her stating that she fantasized of being raped, and providing her address and telephone number. On at least six occasions, sometimes in the middle of the night, men knocked on the woman's door saying they wanted to rape her [4]).

In all of these cases, the software used to commit or enable the Cybercrimes should not be classified as crimeware. In the case of Roger and Hannah, e-mail and instant messaging software was used to do what are normal everyday actions; the sending of e-mail. The student from San Diego crossed the line even further in the commission of his Cybercrime; however, he still did not use crimeware. Finally, the man eventually convicted for stalking and sexual assault used e-mail programs, bulletin board software, and chat clients to post messages, send e-mails and chat – something most of us do every day using the same types of legitimate software he used to commit crime.

Clearly the skill-set needed to investigate Type I Cybercrime differs greatly from the skill-set needed to investigate Type II Cybercrime. Additionally, while there *is* some defense from Type II Cybercrime afforded by technology, the primary defense is currently more human-centric.

5 Topics for future research

This work explores the naturally occurring division between the varied types of Cybercrime. Future research could build on this work by exploring other types of crime that fits, or that could fit, into these divisions. This might give us some insights into what the future of Cybercrime might entail, and by examining both the technical and "people" aspects, it would help us to approach the problem from a more holistic perspective. Compiling a list of program types that would fit under the definition of crimeware would be useful as well. It would be interesting to see how many Cybercrimes actually include crimeware. It is our suspicion that that there are fewer people committing Type I Cybercrimes than is often believed, but that the nature of the crime produces an artificially high estimation of the scope of the problem in terms of perpetrators. It would be interesting to know if similar division occurs in environments that are fully virtual; for example, Second Life.

6 Conclusion

In this paper, we have examined some of the existing definitions of Cybercrime and crimeware, and found there to be significant lack of clarity in their common usage. To address this, we have proposed a more concise definition of these terms, and have further subdivided the area of Cybercrime into two separate areas to facilitate an understanding of the crimes's technological and human dynamic. This understanding is of critical importance, as organizations tasked with defending populations against Cybercrime must begin to at least consider all the crimes within this continuum, and designate appropriate resources to prevent, defend against, and investigate Cybercrime. This is especially important as new laws which address "Cybercrime" begin to take effect at a Federal and State level.

Our definition and separation of cybercrime according to its primary "human" or "not human" factors can be a first step in future research that begins to map these crimes according to a variety of factors. For example, development of a matrix similar to that proposed in earlier Cyberterrorism work could result in an even greater understanding of Cybercrime, possibly enabling researchers to accurately and precisely predict the direction of future Cybercrime. It is to be hoped that by studying Cybercrime with a more holistic perspective, novel solutions to both types of Cybercrime can be created.

Finally, we believe that the situation with Cybercrime and crimeware is rapidly evolving. By attempting to view the problem more inclusively, it should be possible to foresee new developments and take steps toward remediation rapidly. Narrowing or ignoring the problems will create the perfect environment for the Cybercriminal to flourish, undermining the perceived stability and reliability of electronic systems worldwide.

References

1. Bocij, P.: Reactive stalking: a new perspective on victimisation. Br J Forensic Pract **7**(1), 1–5 (2005)
2. Chawki, M.: Cybercrime in France: an overview. Computer Crime Research Center. December, 2005. Downloaded January 23rd 2006 from: http://www.crime-research.org/articles/cybercrime-in-france-overview/ (2005)
3. Davis E., Wright H., Tremaine C.: Beyond phishing: pharming and crimeware attacks. Downloaded Jan 23rd 2006 from: http://www.privsecblog.com/archives/phishingpharming-53-beyond-phishing-pharming-and-crimeware-attacks-.html (2005)
4. DOJ: Cyberstalking: "a new challenge for law enforcement and industry" a report from the Attorney General to the Vice President (August 1999) Downloaded January 23rd 2006 from http://www.usdoj.gov/criminal/cybercrime/cyberstalking.htm. (1999)
5. DOJ: H.R. 3402 Department of Justice Appropriations Authorization Act, fiscal years 2006 through 2009. Downloaded January 23rd from: http://www.gop.gov/Committee-central/bills/hr3402.asp (2005)
6. Gordon, S.: Exploring spyware and adware risk assessment. Presentation to the Computers and Security Institute Conference, Phoenix, Arizona (2005)
7. Gordon, S.: Changing the way the World thinks about computer security. Ph.D. Thesis, University of Middlesex, Department of Computer Science. London, UK (2005)

8. Gordon S., Ford, R.: Cyberterrorism? In: Cybterterrorism. The International Library of Essays in Terrorism, Alan O'Day, Ashgate, ISBN 0 7546 2426 9 (2004)
9. Grodzinsky F.S., Tavani, H.T.: Some ethical reflections on cyberstalking. In: ACM SIGCAS Computers and Society, vol. 32 Issue 1 (2002)
10. Helpguide: Domestic violence and abuse: types, signs, symptoms, Causes, and Effects. A project of the Rotary Club of Santa Monica, California and the Center for Healthy Again. Downloaded January 23rd 2006 from: http://www.helpguide.org/mental/domestic_violence_abuse_types_signs_causes_effects.htm (2005)
11. Informit: Protecting yourself from internet crime. Part II. Downloaded Jan 23rd 2006 from: http://www.informit.com/guides/content.asp?g=security&seqNum=144 (2005)
12. ISTR: Symantec internet security threat report. Trends for July 04 – December 04, Vol VII (2005)
13. Krone T.: High tech crime brief. Australian Institute of Criminology, Canberra, Australia, ISSN 1832–3413 (2005)
14. Kshetri, N.: The simple economics of cybercrimes, security & privacy magazine. In: IEEE, vol. 4, Issue 1, pp. 33–39 (2006)
15. Kuhn, T.: The structure of scientific revolution. 2nd ed. University of Chicago Press, Chicago, Illinois (1992)
16. Parker, D.: Fighting computer crime: a new framework for protecting information ISBN 0471163783. Wiley, New York (1998)
17. PC Magazine: PC magazine encyclopedia. Downloaded Jan 23rd 2006 from: http://www.pcmag.com/encyclopedia_term/0,2542, t=crimeware&i=55434,00.asp (2005)
18. Studycrime: Online resource guide to law and crime. Downloaded Jan 23rd 2006 from: http://www.studycrime.com/Crime/Crimeware.php (2005)
19. United Nations: The united Nations manual on the prevention and control of computer related crime, 1995, supra note 41, paragraphs 20 to 73 in International Review of Criminal Policy, pp. 43–44 (1995)
20. Wikipedia: Common usage crimeware definition. Downloaded Jan 23rd 2006 from http://en.wikipedia.org/wiki/Crimeware (2006)
21. ZD: 2.8 Billion in E-commerce revenues lost to fraud in 2005. ZD Online., Downloaded Jan 23rd 2006 from: http://blogs.zdnet.com/ITFacts/?p=9471 (2005)
22. Zeviar-Geese: The state of the law on cyberjurisdiction and cybercrime on the internet.In: California Pacific School of Law, Gonzaga Journal of International Law, vol. 1 (1997–1998)
23. Zona, M.A., Sharma, K.K., Lane, M.D.: A comparative study of erotomanic and obsessional subjects in a forensic sample. J Forensic Sci **38**, 894–903 (1993)
24. Zona, M.A., Palarea, R.E., Lane, J.C.: (1998). Psychiatric diagnosis and the offender-victim typology of stalking. In Meloy, J.R. The Psychology of Stalking: Clinical and Forensic Perspectives. Academic, San Diego, California: (1998)