Exploring a Warrior Paradigm to Design Out Cybercrime

Mortaza S. Bargh¹, Sunil Choenni¹², Ingrid Mulder¹², and Roland Pastoor¹

¹Creating 010, Rotterdam University of Applied Science
Rotterdam, The Netherlands
{m.shoae.bargh, r.choenni, i.j.mulder, r.m.pastoor}@hr.nl
²Research and Documentation Centre, Ministry of Justice
The Hague, The Netherlands
r.choenni@minjus.nl
³ID-StudioLab, Delft University of Technology
Delft, the Netherlands
i.j.mulder@tudelft.nl

Abstract—Cybercrime increases with the advent of new online Internet services (e.g., entertainment, commerce, payment, public administration, social networking services). Not only do cybercriminals target governmental or public institutions, they increasingly victimize individuals and smaller organizations. At the same time, we observe that individuals and organizations steadily join forces and take a more proactive and collaborative role in war against cybercrime. In the current work we investigate examples of rising security incidents, new information security solutions and new cybercrime legislations, and elaborate upon some mismatches that exist among them. We particularly elaborate upon (the potential of) the collaborative initiatives that allow individuals to join forces and disclose cybercrime threats. We identify and/or outline a number of the research directions in legislation, social and technical arenas.

Keywords-component; collaborative approaches; cybercrime; cybercrime laws; information security solutions; mismatches; research directions; security threats

I. INTRODUCTION

Computers, networks and Internet provide new capabilities and opportunities for users and businesses to interconnect, access information, and execute (a new range of) activities in a fast and easy way. Unfortunately, these new capabilities and opportunities are also available for criminals to carry out their illegal activities. Crime in or via the virtual world, i.e., cybercrime, is referred to an “activity in which computers and networks are a tool, a target, or a place of … criminal activity” [1]. Not only do computers and networks serve as an accelerator for existing types of crime, they enable new types of crime as well. In practice cybercrime is committed by individuals or small groups (disorganized crime), as well as by criminal groups (organized crime). Cybercrime, which impacts individuals, public and private organizations alike, has become a rising concern of nations in this golden era of Internet and cyberspace.

Cybercrime inflicts enormous cost on the society. According to a study carried out by TNO (Netherlands Organization for Applied Scientific Research [2]), cybercrime costs The Netherlands more than 10 billion Euros annually [3]. This amount is about 1.5% till 2% of the country’s GDP (Gross Domestic Product), which is comparable to the country’s economic growth in 2010! According to the study, the largest damage belongs to companies’ intellectual property rights (33%) followed by industrial espionage (20%), tax and social income fraud (15%), extortion and theft of money and personal information (5-10%). Yet there is growing evidence that cybercrime costs increase steadily. According to the Dutch Banking Association (NVB) [4], the Internet banking fraud increased by a factor of 3.5 to 35M€ in 2011, and the skimming fraud (copying payment cards) increased by a factor of 2 to 40M€ in 2011, all compared to those of 2010 [5]. Note that these amounts are just direct costs (i.e., the reimbursements paid to the customers) and do not cover other costs such as indirect costs (i.e., those for upgrading and maintaining of systems) and implicit costs (i.e., those associated with reputation and branding damages). Cybercrime impacts a large number of organizations. Half of the companies in The Netherlands have become victims of cybercrime attacks in 2011, and only 20% of them were able to survive these attacks successfully [6]. Cybercrime causes also nonfinancial damages and puts integrity and reputation of individuals and companies at stake and, at large, impacts online services negatively by making users distrust such services.

Worldwide many research programs are initiated to study cybercrime motives, implications and impacts, and to develop and evaluate effective solutions. A number of survey papers and reports have been written that identify research problems and topics, and show possible solution directions (see, for example, [7] and [8]). Similarly in this paper we present a number of research issues in cybercrime arena. Our contribution, unlike others, focuses on the cybercrime field from the perspective of its victims (i.e., individuals, companies and organizations) and the information systems they use, without divulging technological or criminological aspects. We want to bring up the roles that individuals and organizations take in insurgence of cybercrime, for example: Are users/organizations just cybercrime victims? Do they accept more responsibility in the war against cybercrime? We present a number of solutions and approaches that suggest individuals and organizations must join forces and be collaborators (or warriors) in the fight against cybercrime.
We also point out a number of the mismatches that exist between, on the one side, rising cybercrime threats and, on the other side, the existing tools (i.e., information security systems) and rules (laws and legislations). Ultimately, our objective is to identify and outline a number of research directions in legislation, social and technical arenas that boost the role of users and organizations in combat against cybercrime.

A war against cybercrime in a democratic society is impossible unless there are clear definitions of such crimes and appropriate laws and governance mechanisms to safeguard the rights of all parties. We start our paper with outlining some latest legislative and governance activities against cybercrime and a number of existing inconsistencies (Section 2). Subsequently we discuss how users (Section 3) and organizations (Section 4) are victimized and affected by cybercrime, how they unwillingly contribute to the success of cybercrime (thus, being part of the problem) and how they can help combating cybercrime (thus, being part of a technosocio solution). Sections 2, 3 and 4 do also present a number of research directions for further study. At the end, we draw some conclusions (Section 5).

II. ON CYBERCRIME LAWS AND GOVERNANCE

A. Example Cases

Nowadays we regularly hear about law enforcement authorities exercising and improving their cybercrime monitoring activities. For example, the Energy and Commerce Committee of the US House of Representatives has recently asked Apple Inc. to explain about the company's efforts to protect the privacy and security of its mobile device users [9]. The committee is concerned about the way that apps access photographs on Apple mobile devices and the tools for consumers to prevent unwanted online tracking. As another example, the U.S. Federal Bureau of Investigation (FBI) currently looks for a tool to gather and mine data from blogs and social networks such as Facebook and Twitter [10]. The FBI objective is to know about breaking events, incidents and emerging threats. The FBI wants to use the system only to monitor publicly available information and not to focus on specific individuals or groups. Nevertheless, such measures raise the concerns of privacy protection activists.

Judicial authorities have issued a number of important verdicts against cybercriminals recently. The US department of Justice website [11] enlists a number of such verdicts over a wide range of cybercrimes, for example: denial of service attacks, illegal computer monitoring, botnet computer tampering, bank and credit card fraud, illegal download, production and sell of copyright materials, and stealing the Internet service. Issuing such judicial verdicts demonstrates the determination of the justice system to deal with cybercrimes. There are also judicial actions against ongoing practices of application service providers that pave the way for misuse and crime. For example, the Friend Finder feature of Facebook allows users (even those who are not Facebook members) to input the e-mail addresses of others to the site. Then Facebook uses these address lists and invites their owners to the network. A court in Berlin has recently ruled that this practice of Facebook is unlawful in Germany [12]. It is expected that this court’s rule will be followed in other countries. Nevertheless, there is quite a delay between rolling out such debatable functionalities and legal actions against them [13].

B. Towards the Warrior Paradigm

There are initiatives to setup new laws and legislations to combat cybercrime by relying on a proactive collaboration of involved parties. For example, the Dutch ministry of economic affairs has recently proposed a new law that concerns those parties that collect personal information and, due to some reason, lose their control on this information. Such parties are obliged to report on such information leakage incidents as well as on their countermeasures to the Dutch Data Protection Authority (CBP, het College Bescherming Persoonsgegevens, in Dutch) and to those individuals who have lost their personal information [14]. The objective of the proposal is to increase the risk-awareness of such parties who store sensitive information in high volumes; to encourage them to investigate better the reasons behind data leakages, and to stimulate them to adopt better measures to protect private data. Moreover, when informed on time, individuals can personally take immediate actions to rectify their information breaches such as blocking their bank accounts. As another example, a new European data protection law is being proposed these days that mandates issues like the right to be forgotten [15]. When this proposal becomes legislation, individuals can gain control of and exercise their privacy rights more directly than it is possible nowadays.

C. Issues for Further Study

The introduction of computers and networks went side by side with new possibilities and the creation of new objects. These possibilities and objects have an impact on crime. Computers and networks cause new types of crime, but on the other hand they serve as an accelerator for existing types of crime. For example, swindling is of all time, however, due to the Internet it becomes easier to commit fraud on a larger scale. An illustration of this is the Nigerian fraud.

Our criminal justice system is mainly focused on physical objects. However, computers and networks entail also virtual and hybrid objects, on which crime may be committed. For example, an avatar, which is a virtual object, can be stolen or destroyed. This also holds for hybrid products. A CD (Compact Disk) with an e-learning application is such a product, because the CD itself is a physical object, while the content is a digital product. It is unclear how the law deals with crime committed on these objects. Recently, the Dutch High Court has stated that the theft of an avatar is actionable, since the creation of the avatar requires a significant amount of time and effort.

Concerning the increasing monitoring activities of authorities mentioned in Section II.A, one should also raise the concern of privacy protection activists. An issue for further study is to see which mechanisms are available or needed to maintain an effective oversight and control on
A. Example Cases

A main feeding ground of cybercrime is the personal and private information being scattered in pieces in the Internet. Web shops, Online Social Networks (OSNs), e-government portals, etc. collect personal information about users and citizens. This information includes names, email and postal addresses, dates of birth, geo-locations, social security numbers, bank accounts, photos and opinions. All these sites are vulnerable to some extend to leakage of information. Particularly, OSNs base their business model on sharing (part of) the information that they collect about their users with third parties. These third parties, like the one pointed at [17], enrich the shared information and offer enhanced Web analytics services (for example, traffic measurement, connectivity and geo-location services, user characterization) to other parties such as online advertisement companies. This may stimulate certain types of crime, such as planned burglaries.

Sometimes personal information is directly leaked from their guardians due to an inappropriate or insensitive design. For example, Facebook Places feature raised serious concerns because its default setting allowed a user to tag a friend’s (read someone’s) location and share it without the friend being physically in that location. Such location check-ins could appear in the News Feeds and activity streams for that place, unless otherwise specified [18]. Malicious persons may hereby frame and hurt innocent friends/users by associating them with inappropriate locations.

Often it is possible to link personal information that users leave behind in various virtual sites that they visit. In this way it becomes possible to infer sensitive information about users’ identity, interest, behavior, social contacts, credentials, political views, etc. Such an inference is possible even if measures like de-identification of data (“stripping identity information from data” [19]) are carried out. One can apply re-identification methods to relate information from dispersed data pieces. For example, the authors of [19] describe a method to link de-identified information provided by OSNs with the information provided by web cookies and shows that it is possible to re-identify the OSNs’ profile information. As interestingly stated in [20], nowadays the information available in Facebook is not about our recent profile, but it is about what we have done in that OSN and beyond!

Privacy exposure is not only caused by OSNs’ processing and (partially) sharing of personal information, but is also caused by data breaches at organizations that collect, process and store such information. Hacking of websites and IT systems (for example, see news items [21] [22] and [23]) can compromise private information items like email addresses, credit card numbers, and login credentials. Such exposures allow criminals to carry out various attacks like ID theft attacks (e.g., to use a victim’s bank credentials to withdraw money) and phishing attacks (e.g., to pretend to be a close friend of a victim and do a better social engineering attack against the victim because the criminal knows some private information about him).

B. Towards the Warrior Paradigm

Primarily cybercrime harms individual users by making them, for example, harassed, stalked, accounted for uncommitted crimes, and subject to financial losses. One of the salient impacts of cybercrime on users is users’ fear of crime. The author of [24] argues that our knowledge about the fear of cybercrime is currently too little. It investigates cybercrime victimization to understand users’ Internet behavior “as a reaction to fear of cybercrime” [24]. Negligence and a false perceived sense of security can cause individuals to become victims of cybercrime. Reference [25], for example, reports that most mobile apps that manage the passwords of a user on his smartphone are unsecure. Users use such apps naively (even based on the advice of the IT manager of their organizations) and become subject to and a victim of cyber attacks.

Users also unintentionally contribute to a successful execution of cybercrimes. For example, in OSNs someone can harm others by sharing too much information about them. A well-known example is indiscriminate photo tagging in Facebook, where anybody can add another person’s name to a photo on Facebook. The victim cannot do much about such privacy-violating photo tags [26]. Another example is users harming themselves by recklessly clicking on all interesting links in OSNs. Reference [27] reports that one out of five OSN users clicks on such links and becomes a victim of cybercrime.

Users can also take a proactive role in combating cybercrimes. Raising the awareness of users in their interaction with information systems is a traditional theme in this area. We witness, moreover, a number of solutions that aim at involving users in reducing security risks. Reference [28] considers how to motivate users to be serious about their privacy in OSNs. It considers psychology of ownership to commoditize personal data. Since people are asset-
conscious, in this way they start caring about their private data. Google’s award for experts who find and report vulnerabilities in Google’s web services [16] is another example of relying on collaboration of individuals. Hereby Google encourages individuals (friendly hackers) to join forces and debug the security features of Google’s products. Inline with enabling users to directly report undesirable actions in cyberspace, the authors of [7] propose implementing a “report phishing button” on email clients to report suspicious phishing emails to ISPs (Internet Service Providers).

C. Issues for Further Study

Publically available data (from open data [29], OSNs, etc.) can be used to derive “facts” and statements about citizens and public figures. These facts/statements can be inferred directly or, as in case of large data volumes, by using automatic machine learning methods. It is important to be aware of the subjectivity and uncertainty complications of such inferences, particularly considering the fact the web has a “never forget” tendency (which makes minor misinterpretations to “live on forever”) [30]. The authors of [31] argue that in using data mining and machine learning techniques we adopt a number of assumptions about the data (e.g., in transforming content to data, choosing the learning algorithm, generalization of the results). Each of such assumptions may significantly impact the final inferred outcomes. Such a bias towards data should be assessed and “reported” at the outset, especially in interdisciplinary works, in order to prevent a distorted artifact or a picture being mistaken for an underlying truth [31]. Specially, in [32] the authors argue that mining of the data that partly comes from legacy databases may result in knowledge that might have been true in the past but is not necessarily true today. It is of great importance to investigate the ways of making appropriate assumptions about data and conveying these assumptions together with the (privacy sensitive) outcomes of an inference process to the public or authorities.

On victimization of users it is necessary to investigate the diverse impacts of cybercrime on different types of users (e.g., old, young, man, woman), and on their online behavior, especially if they are misled by a perceived sense of security. An answer to this question, e.g., a cybercrime model of user groups, allows us to have a realistic assessment about the risks associated with such crimes. In case of users unknowingly and unwillingly assisting cybercriminals, one should investigate how users can also be taken into account in modeling vulnerabilities of information systems and how effective such human-technical models are in risk assessment and treatment. Concerning users’ collaboration for combating cybercrime, the challenge is to find new application areas and effective mechanisms for capitalizing user crowds. Hereto it is interesting to see how ICT can support users in collaborative defending of (their) information assets.

IV. On Cybercrime and Organizations

A. Example Cases

Small, middle and large sized organizations are also victims of cybercrime. In April 2011, Sony discovered that hackers had attacked and gained unauthorized access to its PlayStation Network (PSN) servers. In this attack personal information of about 77 million PSN customers may have been stolen. A few days later, another 24 million user accounts were exposed to hackers in Sony Online Entertainment (SOE) system. A few weeks later network intruders accessed user accounts in Sony mobile Internet service provider in Japan and subsequently hacked 2,000 Sony Ericsson mobile users in Canada [33]. The stolen information items included: name, address (city, state, zip, country), email address, gender, birthdate, phone number, login name and hashed password. Moreover, about 10,700 outdated direct debit records (bank account number, customer name, account name, customer address) were stolen from accounts in Austria, Germany, Netherlands and Spain [34].

Other security breaches at companies’ and organizations’ sites that have appeared in news recently include: leakage of clients’ credentials due to hacking of a webhost provider [35], leakage of client emails and login information due to hacking of websites [36] (70,00 accounts), [37] (2.3 million accounts), and [38] (between 150,000 and 318,000 email addresses). Cybercriminals also hack websites of organizations for, for example, pleasure, showoff, and making (political) statements (e.g., hacking the websites of Vatican [39] and British Home Office [40]).

B. Towards the Warrior Paradigm

Primarily organizations, companies, and institutes are victims of cybercrime. For many years organizations and commercial companies try to develop a great brand name with a reputation of quality. Cybercrime attacks can, unfortunately, ruin all these efforts in a short period of time. In the example of Sony mentioned above, the hacking of PSN and SOE put the networks offline for a few weeks. An even greater concern was the potential financial impact because of customers becoming hesitant to use any of Sony’s online services (i.e., implicit costs of cybercrime). Recently a data breach occurred at Global Payments, a payments processing firm that processes card transactions. The company confirmed on March 30, 2012 that credit and debit card information from major card brands might have been accessed. A Wall Street Journal report about Global Payments being hacked sent the company’s shares down 9% on the same day [41]! This shows how fast and how severe cybercrime can cause financial impacts on companies. Cybercrime can even bring a company to bankruptcy as it did so in the case of Dutch DigiNotar [42].

Organizations may also contribute to a successful execution of cybercrime unintentionally. Reference [43], for example, reports on a security leakage (due to a SQL (Structured Query Language) injection attack) in the website of a company that made 125 other websites, residing on the same webserver, vulnerable. Another example is the spread
of a malware via the site of nu.nl, which is the most visited news website in The Netherlands. The site’s visitors were infected by the malware in the short time interval that a cybercriminal gained access to the site’s CMS (Content Management System) and infected it with the malware [44]. Such examples show how vulnerability in the information system of one organization makes others also vulnerable in cyberspace. This can be due to, among others, complex dependencies and unforeseeable relationships.

Nowadays we witness new initiatives that encourage organizations to take a proactive and collaborative role in the struggle against rising cybercrimes. For example, in the keynote speech of the RSA 2012 conference FBI director Robert Mueller mentioned that every company will be a victim of cybercrime sooner or later and he asked for collaboration of companies with the government in reporting cybercrime incidents [45]. The Dutch government has also advocated such an approach [14], as explained in Section II.B. Recently distributed defense approaches and collaborative security technologies have gained interest due to their manageability, reduced operating costs and architectural simplicity. Such approaches are based on sharing information for accelerating detection of and response to new attacks and threats and sharing resources for increasing the resource consumption efficiency. For example, authors of [46] propose maintaining a black list of fake sites by using smart crowdsourcing techniques and authors of [47] propose sharing network attack graphs among multiple ISPs.

C. Issues for Further Study

Trust is an important commodity in business and trade. It is also an important aspect of relationships between people. When one is vulnerable to harm from someone else but believes that the other one will not harm him (although he could), then that is a matter of trust. Brick and mortar organizations put a lot of efforts to gain and to retain trust. A wide variety of means is deployed to minimize the harm we risk and to maximize the good we expect from the business. For example, branding and providing guarantee on a product are used to increase the trust in the product. Trust is actually always a trade-off between benefits and risks for an organization. Betrayal or lack of trust jeopardizes the relationship that customers have with organizations. Brick and mortar organizations have one or more registered offices with clear addresses. Customers may visit these offices, whenever they feel to do so. A visit to such an office may increase the trust in an organization. It also may happen that a customer is disappointed by the visited site for different reasons and decides not to do business with this organization. Therefore, organizations spend efforts in organizing their registered sites in such a way that it helps to increase the trust of customers. In case of “virtual” organizations, however, there are no registered offices with physical addresses that are used to receive a large number of customers. Furthermore, virtual organizations may be physically seated far away from their customers, and can be therefore almost unreachable or difficult to reach for a personal visit. This may have a consequence that virtual organizations are more vulnerable for trust compared to brick and mortar organizations for two reasons. First, the chance that customers become suspicious in the case of bad experiences is higher compared to bad experiences with brick and mortar organizations. This is simply because they cannot visit a site to convince themselves that their experience was just an incident. Second, people who want to cause damage to a virtual organization may post massive bad reviews of this organization. Consequently, the trust in the virtual organization may decrease, since customers have hardly the opportunity to visit a site of the organization to convince themselves of the opposite. In order to gain trust, today, many organizations guarantee their customers that they will be compensated for losses due to cybercrime. However, if these losses grow exponentially and exceed a certain amount, the question raises how long organizations will preserve such guarantees. Therefore, for virtual organizations we should look for sustainable solutions, mechanisms and means that compensate the lack of a physical office.

Every organization normally investigates and estimates divers socio-economical impacts of information security breaches on its information systems and core businesses as part of a risk management process. This is (or must be) an iterative and continuous process. Steadily cybercrimes become more sophisticated and occur more frequently. On the other hand, when a large company becomes subject to cyber attacks (remember the example of Sony in Section IV.A), next to the company’s reputation and online services, other companies’ online services and businesses might be affected negatively. Such cross-organizational (or macro) impacts of cybercrime originate from damaged customer trust at large. Consequently organizations should investigate how new cybercrimes evolve and capture/assess also the macro impacts of such crimes on their organizations and business processes. Hereby they can have a realistic assessment about the risks associated with expected cybercrimes.

Vulnerability in the information system of one organization may make others also vulnerable in cyberspace due to, among others, complex dependencies and unforeseeable relationships among organizations. A relevant research question is how we can model or take into account such complex dependencies in modeling cyber attacks. Other related questions are how and how much an ignorant organization can be considered accountable if it unintentionally jeopardizes or compromises the security of other organizations and users.

Considering the move towards the warrior paradigm, we foresee a number of research questions such as which collaborative approaches among organizations (like ISPs) are possible, how effective they are, what their consequences are in terms of, e.g., privacy and trade secrecy; and finally how technology and technical solutions can support their effective implementations.

V. DISCUSSION AND CONCLUSIONS

In this contribution we investigated a number of recent cybercrime incidents and considered the roles of individuals
and organizations in the insurgency of cybercrime. These example incidents show that individuals and organizations are not just victims of cybercrime. They do also introduce vulnerability to the information systems of theirs and others. Therefore we enlisted a number of research questions on socio-technical and cross-organizational modeling of cyber threats, which are informing our future research on designing out cybercrime.

Furthermore, we outlined a number of collaborative approaches wherein individuals and organizations assume a more proactive role to combat cybercrime. Based on these observations and also inspired by the success of Web 2.0 and crowdsourcing concepts, we foresee the increasing rise of the so-called “warrior paradigm” according to which individuals collaborate proactively to form the first line of defense against cybercrime. This can be considered as a paradigm shift: from being victims of cybercrime to becoming warriors against cybercrime. Here to we mentioned a number of research directions.

Our criminal justice system is mainly focused on physical objects. As computers and networks entail also virtual and hybrid objects on which crime may be committed, we think a substantial research efforts must be invested in crystallizing how the law should deal with crime committed on these objects. The task of establishing and maintaining trust is more challenging for virtual organizations compared to that for organizations with physical sites. Therefore in case of virtual organizations we should look for solutions and mechanisms that compensate the lack of a physical office in establishing and maintaining of trust. Differently stated, both physical and virtual aspects need to be addressed in order to design out cybercrime.

In our future work we use a designerly approach to cybercrime. Here, we elaborate upon Ekblom’s framework on the conjunction of criminal opportunity [48]. Currently there is not enough attention paid to evaluation of the impacts of cybercrime intervention mechanisms [49]. We will start our work with investigating how the “stated-preference” method can be applied (a) to model the behavior of a cybercrime such as digital piracy (i.e., downloading and uploading of digital objects) and (b) to measure the impacts of the existing or new intervention mechanisms against digital piracy. Developing such a method will enable us to identify and/or develop effective intervention mechanisms. We envision that collaborative mechanisms have a great potential to alleviate cybercrime. Consequently we will consider distributed cybercrime defense mechanisms and tools that involve end users to collaboratively detect and deal with cyber-attacks.

REFERENCES


